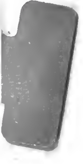
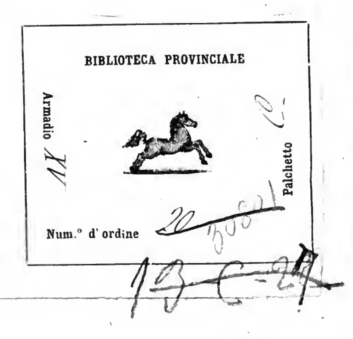

BIBLIOTECA DI ARTIGLIERIA


FONDO PIZZOFALCONE




BIBLIOTECA PROVINCIALE
Armadio XV
Palchetto C
Num.° d' ordine 20
13-C-24



COURS

D'ALGÈBRE SUPÉRIEURE.

LIBRAIRIE DE BACHELIER.

Cet ouvrage se trouve aussi

A BORDEAUX... chez CHAUMAS.
LILLE...... — VANACKÈRE.
LYON...... { — PERISSE frères.
— BRUN et Cie.
MARSEILLE... — Mme Vve CAMOIN.
METZ........ — WARION.
MONTPELLIER. — SÉWALLE.
NANCY....... — G. GRIMBLOT et Cie.
NANTES..... { — FOREST aîné.
— GUÉRAUD.
ORLÉANS..... — GATINEAU.
RENNES...... — VERDIER.
ROUEN....... — LEBRUMENT.
STRASBOURG. { — TREUTTEL et WURTZ.
— Mme LEVRAULT.
— DERIVAUX.
TOULOUSE.... { — Mlles GALLON sœurs.
— PRIVAT.
— GIMET.

AMSTERDAM.... chez VAN BAKKENES.
BERLIN....... — B. BEHR.
BRUXELLES.... { — DECQ.
— PÉRICHON.
CAMBRIDGE.... — DEIGTON.
COPENHAGUE... — HOST.
FLORENCE..... — PIATTI.
GÊNES....... — BEUF.
GENÈVE...... — CHERBULIEZ.
LA HAYE...... — VAN CLEEF frères.
LEIPSIG....... — MICHELSEN.
LONDRES...... — BAILLIÈRE.
MADRID....... { — Mme POUPART et frère.
— JAYMEBON et Cie.
— MONIER.
ROME........ — BLEGGI.
NAPLES....... — GAETANO NOBILE.
TURIN........ — BOCCA.

Imprimerie de BACHELIER, rue du Jardinet, 12.

COURS

D'ALGÈBRE SUPÉRIEURE,

PROFESSÉ

A LA FACULTÉ DES SCIENCES DE PARIS;

Par J.-A. SERRET,
Examinateur pour l'admission à l'École Polytechnique.



PARIS,
BACHELIER, IMPRIMEUR-LIBRAIRE
DE L'ÉCOLE POLYTECHNIQUE, DU BUREAU DES LONGITUDES, ETC.,
QUAI DES AUGUSTINS, 55.

1849







AVERTISSEMENT.

Cet Ouvrage est le résumé des Leçons que j'ai professées à la Sorbonne, dans la Chaire que la Faculté des Sciences m'a fait l'honneur de me confier cette année (1848).

Entièrement libre du choix des matières de mon Cours, j'ai développé la théorie de la résolution algébrique des équations, et les questions incidentes qui s'y rattachent. Je crois n'avoir omis aucun des faits principaux acquis à cette partie de la science.

La connaissance de l'Algèbre élémentaire, telle qu'elle est exposée dans l'excellent ouvrage de M. Lefébure de Fourcy, suffit pour l'intelligence des théories les plus importantes de ce livre. Toutefois, j'ai cru pouvoir faire usage du calcul différentiel et du calcul intégral, dans un petit nombre de passages.

Ces rédactions n'avaient pas été d'abord destinées

à l'impression : en les publiant, j'ai cédé au vœu exprimé par MM. les Professeurs qui m'ont fait l'honneur de suivre mon Cours. Je m'estimerai heureux si je contribue, par là, à propager l'étude d'une des parties les plus intéressantes et les moins connues de l'analyse.

TABLE DES MATIÈRES.

PREMIÈRE LEÇON.

DEUXIÈME LEÇON.

TROISIÈME LEÇON.

QUATRIÈME LEÇON.

CINQUIÈME LEÇON.

SIXIÈME LEÇON.

SEPTIÈME LEÇON.

HUITIÈME LEÇON.

NEUVIÈME LEÇON.

DIXIÈME LEÇON.

ONZIÈME LEÇON.

DOUZIÈME LEÇON.

TREIZIÈME LEÇON.

QUATORZIÈME LEÇON.

QUINZIÈME LEÇON.

SEIZIÈME LEÇON.

DIX-SEPTIÈME LEÇON.

DIX-HUITIÈME LEÇON.

DIX-NEUVIÈME LEÇON.

VINGTIÈME LEÇON.

VINGT ET UNIÈME LEÇON.

VINGT-DEUXIÈME LEÇON.

VINGT-TROISIÈME LEÇON.

VINGT-QUATRIÈME LEÇON.

VINGT-CINQUIÈME LEÇON.

VINGT-SIXIÈME LEÇON.

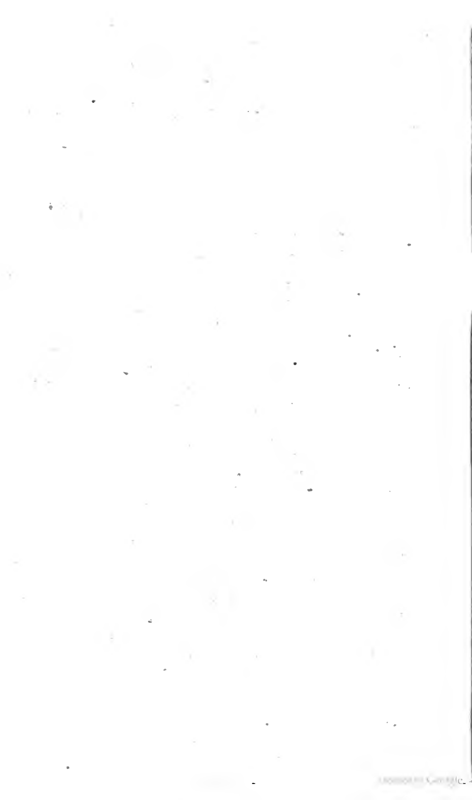
VINGT-SEPTIÈME LEÇON.

VINGT-HUITIÈME LEÇON.

VINGT-NEUVIÈME LEÇON.

TRENTIÈME LEÇON.

FIN DE LA TABLE DES MATIÈRES.



COURS
D'ALGÈBRE SUPÉRIEURE.

PREMIÈRE LEÇON.

Introduction. — Des fonctions symétriques. — Détermination des sommes de puissances semblables des racines d'une équation.

Introduction.

L'Algèbre est, à proprement parler, l'*Analyse des équations;* les diverses théories partielles qu'elle comprend se rattachent toutes, plus ou moins, à cet objet principal. A ce point de vue, l'Algèbre peut se diviser en trois parties bien distinctes :

1°. *La théorie générale des équations*, c'est-à-dire l'ensemble des propriétés qui sont communes à toutes les équations;

2°. *La résolution des équations numériques*, c'est-à-dire la détermination des valeurs exactes ou approchées des racines d'une équation dont les coefficients sont donnés en nombres;

3°. *La résolution algébrique des équations*, c'est-à-dire la détermination d'une expression composée avec les coefficients d'une équation donnée, et qui, substituée à l'inconnue, satisfasse identiquement à cette équation, soit que les coefficients de l'équation proposée soient *numériquement donnés*, soit qu'étant simplement considérés comme connus, ils restent indéterminés et représentés par des lettres.

Je me propose, dans ce Cours, d'exposer spécialement les recherches que les géomètres ont entreprises jusqu'à

nos jours *sur la résolution algébrique des équations*, en admettant comme connues les *propriétés générales des équations*, et la plupart des principes sur lesquels repose leur résolution numérique. Je me réserve, toutefois, de revenir sur quelques points principaux de ces deux théories, qui se rattachent à l'objet de nos investigations.

Sans prétendre faire ici l'histoire complète de l'Algèbre, je crois devoir, dès à présent, donner un aperçu des principaux résultats acquis à cette partie de la science que nous allons étudier.

Il serait difficile de dire à qui nous devons la résolution des équations du second degré; elle se trouve dans le livre de Diophante, et, comme le fait remarquer Lagrange dans son *Traité de la Résolution des équations numériques*, elle ressort naturellement de quelques propositions d'Euclide. Luc Paciolo, qui publia en 1494, à Venise, le premier livre d'Algèbre paru en Europe, ne fait aucune mention de Diophante, et laisse supposer que les algébristes italiens avaient appris des Arabes ce qu'ils savaient d'algèbre, c'est-à-dire la résolution des équations du premier et du second degré.

La résolution des équations du troisième degré est due à deux géomètres italiens du XVIe siècle, Scipion Ferrei et Tartaglia; mais on ignore par quel chemin ils y ont été conduits, et la formule qui représente les trois racines de l'équation du troisième degré est communément appelée la *formule de Cardan*.

C'est aussi à un géomètre italien, Louis Ferrari, disciple de Cardan, que l'on doit la résolution de l'équation du quatrième degré. Depuis, plusieurs méthodes, que nous indiquerons successivement, ont été proposées pour la résolution des équations du troisième et du quatrième degré; mais Lagrange a montré, dans un excellent Mémoire inséré parmi ceux de l'Académie de Berlin,

pour 1770 et 1771, que ces méthodes, différentes en apparence, reviennent toutes, au fond, à faire dépendre la résolution de l'équation proposée, de celle d'une seconde équation qu'il appelle *résolvante*, et dont la racine est composée linéairement avec celles de la proposée et les puissances d'une racine de l'unité du même degré. En cherchant à généraliser cette méthode, à l'étendre aux équations de tous les degrés, ce grand géomètre a montré qu'au delà du quatrième degré, l'équation résolvante était d'un degré supérieur à celui de la proposée, et ne paraissait pas, en général, susceptible d'abaissement. Il a enfin fait voir clairement, par cette analyse, à quelle circonstance est due la résolution générale des équations des quatre premiers degrés, circonstance qui ne se présente plus au delà du quatrième degré.

Toutefois, Lagrange a appliqué sa méthode avec le plus grand succès à la résolution des équations binômes de tous les degrés; résolution que M. Gauss avait effectuée le premier, par une méthode ingénieuse fondée sur les relations qui existent entre les diverses racines de l'équation binôme, et sur la considération des *racines primitives* des nombres premiers.

Abel, en généralisant l'analyse de M. Gauss, a montré ensuite que si deux racines d'une équation *irréductible* sont tellement liées entre elles, que l'une puisse s'exprimer rationnellement par l'autre, l'équation est soluble par radicaux, si son degré est un nombre premier, et que, dans le cas contraire, sa résolution dépend de celle d'équations de degrés moindres que le sien. C'est là un des plus beaux résultats dont l'Algèbre se soit enrichie de nos jours. Abel a fait, dans son Mémoire, l'application de sa méthode à l'équation binôme, et a notablement simplifié la marche suivie par M. Gauss.

Voici donc une classe assez étendue d'équations dont

les racines peuvent être exprimées par radicaux; mais ces équations, étudiées par Abel, sont-elles les seules qui possèdent cette propriété? Dans quel cas, en un mot, une équation peut-elle être résolue algébriquement? Cette question difficile a été résolue complétement, au moins pour les équations irréductibles de degré premier, par Évariste Gallois, ancien élève de l'École Normale, et l'un des géomètres les plus profonds que la France ait produits. Dans un Mémoire présenté à l'Académie des Sciences en 1831, et publié en 1846 par les soins de M. Liouville, Gallois a, en effet, démontré ce beau théorème : *Pour qu'une équation irréductible de degré premier soit soluble par radicaux, il faut et il suffit que, deux quelconques des racines étant données, les autres s'en déduisent rationnellement.*

Enfin, quant aux équations dont les racines sont des quantités quelconques n'ayant entre elles aucune dépendance, c'est-à-dire dont les coefficients restent indéterminés, leur résolution générale est impossible au delà du quatrième degré. Cette proposition importante, énoncée par Ruffini, a été mise hors de doute par les travaux plus récents d'Abel.

Tels sont les travaux les plus importants qui aient été entrepris sur la résolution algébrique des équations, et dont j'ai cru devoir faire ici l'indication succincte.

Nous commencerons ce Cours par l'exposition d'une théorie fort simple, des principes de laquelle nous ferons un usage fréquent, et que, pour cette raison, je crois devoir rappeler avec quelques détails; je veux parler de la théorie des fonctions symétriques.

Des fonctions symétriques.

Une fonction de deux ou plusieurs quantités est dite *symétrique*, lorsque sa valeur n'est pas changée par les

diverses permutations des quantités qu'elle renferme; nous ne nous occuperons ici que des fonctions symétriques *rationnelles*.

Les coefficients d'une équation sont des fonctions symétriques des racines de cette équation; ce sont même les fonctions symétriques les plus simples, puisque chaque racine n'y entre qu'au premier degré.

On aperçoit facilement que *toute fonction rationnelle et symétrique des racines d'une équation peut s'exprimer rationnellement à l'aide des coefficients de cette équation.*

Car, soit l'équation

$$x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0.$$

En désignant par $a, b, c, \ldots, k, l$ ses m racines, on a les relations connues

$$(1)\quad \begin{cases} a + b + c + \ldots + k + l = -p_1, \\ ab + ac + \ldots\ldots\ldots\ldots = p_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ abc\ldots kl = \pm p_m; \end{cases}$$

si, en outre, on désigne par V une fonction symétrique et rationnelle des m racines, en sorte qu'on ait

$$(2)\qquad V = F(a, b, c, \ldots, k, l),$$

et qu'on élimine les m racines $a, b, \ldots, k, l$ entre les équations (1) et (2), on aura une équation en V qui ne pourra être que du premier degré, puisque la quantité V n'a qu'une seule valeur; par suite, V s'exprimera rationnellement par les quantités p_1, p_2, etc. En général, si la quantité désignée par V est susceptible de μ valeurs différentes, lorsqu'on fait subir aux lettres a, b, c, etc., toutes les permutations possibles, l'équation en V résultant de l'élimination de a, b, c, etc., entre les équations (1) et (2), sera évidemment du degré μ.

Nous allons montrer comment on peut trouver l'expression d'une fonction symétrique et rationnelle quelconque des racines d'une équation, et cette recherche nous conduira à une démonstration nouvelle plus précise et plus claire du théorème que nous venons de démontrer. Examinons d'abord à quoi peut se réduire la recherche de la fonction symétrique et rationnelle la plus générale possible. Toute fonction rationnelle non entière est le quotient de deux fonctions entières, en sorte qu'il n'y a lieu de s'occuper que des fonctions symétriques entières. En outre, toute fonction symétrique entière non homogène est la somme de deux ou plusieurs fonctions symétriques homogènes; tout est donc ramené à établir des règles pour calculer les fonctions symétriques rationnelles entières et homogènes; enfin, une pareille fonction symétrique entière et homogène peut contenir des termes où les exposants des lettres, tout en ayant la même somme, ne soient pas égaux chacun à chacun : dans ce cas, la fonction est la somme de deux ou d'un plus grand nombre de fonctions symétriques de même degré, mais différentes, et que nous calculerons séparément. De tout cela, il résulte que nous pourrons nous borner à la détermination des fonctions symétriques rationnelles, entières et homogènes, telles que les exposants des lettres soient les mêmes dans deux termes quelconques. Toute fonction de cette espèce sera déterminée si l'on connaît un seul de ses termes, ainsi que toutes les lettres qui entrent dans sa composition. Cela posé, nous appellerons *fonction symétrique simple ou du premier ordre*, une fonction symétrique rationnelle, entière et homogène, dont chaque terme ne contient qu'une seule lettre; *fonction symétrique double ou du deuxième ordre*, celle dont chaque terme renferme deux lettres, et ainsi de suite.

Détermination des sommes de puissances semblables des racines d'une équation.

Soit l'équation

$$x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0,$$

que nous représenterons aussi, pour abréger, par

$$X = 0,$$

et dont nous désignerons par $a, b, c, \ldots, k, l$ les m racines. Soit, en outre, X' le polynôme dérivé de X, on aura

$$X' = m x^{m-1} + (m-1) p_1 x^{m-2} + \ldots + 2 p_{m-2} x + p_{m-1}.$$

On a aussi, par un théorème connu,

$$X' = \frac{X}{x-a} + \frac{X}{x-b} + \ldots + \frac{X}{x-l};$$

et l'on trouve, par la division,

$$\frac{X}{x-a} = x^{m-1} + \begin{array}{l|l|l|l} a & x^{m-2} + a^2 & x^{m-3} + a^3 & x^{m-4} + \ldots + a^{m-1} \\ + p_1 & \quad + p_1 a & \quad + p_1 a^2 & \quad + p_1 a^{m-2} \\ & \quad + p_2 & \quad + p_2 a & \quad + p_2 a^{m-3} \\ & & \quad + p_3 & \quad + \ldots\ldots \\ & & & \quad + \ldots\ldots \\ & & & \quad + p_{m-2} a \\ & & & \quad + p^{m-1}. \end{array}$$

Si, dans cette équation, on remplace successivement a par chacune des autres racines, et qu'on fasse généralement

$$s_n = a^n + b^n + c^n + \ldots + k^n + l^n,$$

on aura, en ajoutant tous les résultats, la valeur suivante

de X',

$$\begin{array}{l|l|l|l}
X' = mx^{m-1} + s_1 & x^{m-2} + s_2 & x^{m-3} + s_3 & x^{m-4} + \ldots + s_{m-1} \\
\quad + mp_1 & \quad + p_1 s_1 & \quad + p_1 s_2 & \quad + p_1 s_{m-2} \\
 & \quad + mp_2 & \quad + p_2 s_1 & \quad + p_2 s_{m-3} \\
 & & \quad + mp_3 & \quad + \ldots\ldots \\
 & & & \quad \ldots\ldots \\
 & & & \quad \ldots\ldots \\
 & & & \quad + p_{m-2} s_1 \\
 & & & \quad + mp_{m-1}.
\end{array}$$

La comparaison de cette valeur de X' avec celle écrite plus haut, fournit les relations suivantes :

$$(1)\left\{\begin{array}{l}
s_1 + p_1 = 0, \\
s_2 + p_1 s_1 + 2p_2 = 0, \\
s_3 + p_1 s_2 + p_2 s_1 + 3p_3 = 0, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
s_{m-1} + p_1 s_{m-2} + p_2 s_{m-3} + \ldots + p_{m-2} s_1 + (m-1) p_{m-1} = 0.
\end{array}\right.$$

La première de ces équations fait connaître s_1 ou la somme des racines, la seconde fait connaître s_2 ou la somme de leurs carrés, et ainsi de suite, jusqu'à la dernière qui fait connaître s_{m-1}.

Voici maintenant comment on peut former les sommes de puissances semblables, dont le degré surpasse $m - 1$, et celles dont le degré est négatif. Soit n un nombre entier positif, nul ou négatif, et multiplions l'équation proposée par x^n ; elle deviendra

$$x^{m+n} + p_1 x^{m+n-1} + p_2 x^{m+n-2} + \ldots + p_{m-1} x^{n+1} + p_m x^n = 0.$$

Remplaçons successivement x par chacune des racines a, b, c, etc., et ajoutons tous les résultats ; on aura

$$s_{m+n} + p_1 s_{m+n-1} + p_2 s_{m+n-2} + \ldots + p_{m-1} s_{m+1} + p_m s_n = 0 ;$$

en donnant à n les valeurs 0, 1, 2, etc., et observant

que $s_0 = m$, on obtiendra les relations suivantes :

$$(2)\left\{\begin{array}{l} s_m + p_1 s_{m-1} + p_2 s_{m-2} + \ldots + p_{m-1} s_1 + m p_m = 0, \\ s_{m+1} + p_1 s_m + p_2 s_m + \ldots + p_{m-1} s_2 + p_m s_1 = 0, \\ s_{m+2} + p_1 s_{m+1} + p_2 s_m + \ldots + p_{m-1} s_3 + p_m s_2 = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}\right.$$

Les sommes $s_1, s_2, \ldots, s_{m-1}$ étant connues par les équations (1), la première des équations (2) déterminera s_m, la seconde s_{m+1}, et ainsi de suite. Il importe de remarquer que les valeurs des sommes s_1, s_2, etc., ne contiendront, dans leur expression, aucun dénominateur, et que si les coefficients p_1, p_2, etc., sont des nombres entiers, les sommes s_1, s_2, etc., le seront également.

Réciproquement, si l'on connaît m sommes de puissances semblables, par exemple $s_1, s_2, \ldots, s_m$, on pourra déterminer les coefficients p_1, p_2, etc., à l'aide des équations (1) et (2), qui ont été données, pour la première fois, par Newton.

On calculera aussi aisément les sommes de puissances semblables des racines à exposants négatifs, en donnant au nombre n, que nous avons introduit, les valeurs successives -1, -2, -3, etc.; mais à l'égard de ces sommes de puissances négatives, le moyen le plus facile de les trouver, consiste à changer x en $\frac{1}{x}$ dans l'équation proposée, et à calculer ensuite les sommes de puissances semblables à exposants positifs, des racines de cette transformée.

Autre méthode. — On peut employer une autre méthode pour calculer les sommes des puissances semblables des racines d'une équation ; cette seconde méthode a l'avantage de n'exiger qu'une simple division algébrique. Soit toujours

$$X = 0$$

une équation ayant pour racines $a, b, c, \ldots, k, l$. Si X' représente la dérivée de X, on a, comme précédemment,

$$\frac{X'}{X} = \frac{1}{x-a} + \frac{1}{x-b} + \ldots + \frac{1}{x-l}.$$

D'ailleurs,

$$\frac{1}{x-a} = \frac{1}{x} + \frac{a}{x^2} + \frac{a^2}{x^3} + \ldots;$$

donc, en remplaçant successivement a par chacune des autres racines, et ajoutant ensemble tous les résultats, on aura

$$\frac{X'}{X} = \frac{m}{x} + \frac{s_1}{x^2} + \frac{s_2}{x^3} + \ldots,$$

ou

$$\frac{xX'}{X} = m + \frac{s_1}{x} + \frac{s_2}{x^2} + \ldots.$$

Pour le calcul numérique, il sera plus commode d'éviter les exposants négatifs : on changera alors x en $\frac{1}{z}$, et la fraction $\frac{xX'}{X}$ sera de la forme $\frac{Z_1}{Z}$; on aura

$$\frac{Z_1}{Z} = m + s_1 z + s_2 z^2 + \ldots,$$

et l'on obtiendra toutes les sommes s_1, s_2, etc., par la simple division des polynômes Z_1 et Z que l'on ordonnera par rapport aux puissances croissantes de z.

Exemple. — Soit l'équation $X = x^3 - 7x + 7 = 0$; on aura

$$\frac{Z_1}{Z} = \frac{xX'}{X} = \frac{3x^3 - 7x}{x^3 - 7x + 7} = \frac{3 - 7z^2}{1 - 7z^2 + 7z^3},$$

et l'on trouve, par la division,

$$\frac{3 - 7z^2}{1 - 7z^2 + 7z^3} = 3 + 14z^2 - 21z^3 + 98z^4, \ldots,$$

d'où

$$s_1 = 0, \quad s_2 = 14, \quad s_3 = -21, \quad s_4 = 98, \ldots.$$

DEUXIÈME LEÇON.

Détermination des fonctions symétriques doubles, triples, etc., des racines d'une équation. — Formation de l'équation d'où dépend une fonction rationnelle et non symétrique des racines d'une équation donnée. — Équation aux carrés des différences. — Sur la forme des fonctions rationnelles d'une ou de plusieurs racines d'une équation.

Détermination des fonctions symétriques doubles, triples, etc., des racines d'une équation.

Les formules, dues à Newton, que nous avons établies dans la leçon précédente, permettent de calculer très-aisément les fonctions symétriques doubles, triples, etc., des racines d'une équation.

Soient $a, b, c, \ldots, k, l$ les m racines d'une équation $X = 0$ de degré m, et considérons une fonction symétrique double, dont un terme soit $a^p b^q$; la fonction dont il s'agit, étant déterminée quand on en connaît un terme, nous la représenterons, pour abréger, par $\sum a^p b^q$, et nous continuerons de désigner par s_p la somme des puissances $p^{\text{ièmes}}$ de toutes les racines.

Cela posé, si l'on multiplie entre elles les deux sommes s_p et s_q, on voit aisément que le produit sera la somme des deux quantités s_{p+q} et $\sum a^p b^q$; on aura donc

$$\sum a^p b^q = s_p s_q - s_{p+q}.$$

Toute fonction double $\sum a^p b^q$ sera donc exprimable

sous forme rationnelle et entière, à l'aide des coefficients de l'équation proposée, puisque s_p, s_q et s_{p+q} le sont; et si les coefficients de l'équation sont des nombres entiers, $\sum a^p b^q$ sera aussi un nombre entier.

La formule précédente n'a plus lieu si $q=p$; on voit, en effet, que si q devient égal à p, les termes de $\sum a^p b^q$ sont égaux deux à deux, en sorte que cette quantité se réduit à $2\sum a^p b^p$; on aura donc

$$\sum a^p b^p = \frac{1}{2}\left[(s_p)^2 - s_{2p}\right].$$

En remplaçant s_p et s_{2p} par leurs valeurs, on aura la valeur de $\sum a^p b^p$ qui ne contiendra plus le dénominateur 2, mais cela ne se voit pas immédiatement; cette proposition résultera, comme nous le verrons dans la prochaine leçon, d'une nouvelle méthode due à M. Cauchy, pour la détermination des fonctions symétriques des racines d'une équation.

Une fonction symétrique triple, dont un terme est $a^p b^q c^r$, pourra être représentée par $\sum a^p b^q c^r$. Si l'on multiplie la fonction double $\sum a^p b^q$, que nous savons former par s_r, on trouvera pour produit

$$\sum a^p b^q c^r + \sum a^{p+r} b^q + \sum a^p b^{q+r};$$

on aura donc

$$\sum a^p b^q c^r = s_r \sum a^p b^q - \sum a^{p+r} b^q - \sum a^p b^{q+r}.$$

Cette formule fait connaître la fonction triple $\sum a^p b^q c^r$, car le second membre ne contient que des fonctions doubles que l'on sait calculer. Si l'on veut avoir la valeur de la fonction triple, à l'aide de sommes de puissances semblables, il suffira de remplacer les fonctions doubles par leurs valeurs connues; on trouvera ainsi

$$\sum a^p b^q c^r = s_p\, s_q\, s_r - s_{p+q}\, s_r - s_{p+r}\, s_q - s_{q+r}\, s_p + 2 s_{p+q+r},$$

et l'on voit que les fonctions triples s'exprimeront comme les fonctions simples et doubles, sous forme rationnelle et entière, à l'aide des coefficients de l'équation proposée.

La relation précédente n'a plus lieu, si deux des exposants ou tous les trois deviennent égaux entre eux; mais on peut en déduire aisément les valeurs des deux fonctions

$$\sum a^p b^p c^r \quad \text{et} \quad \sum a^p b^p c^p.$$

On voit, en effet, que si q devient égal à p, $\sum a^p b^q c^r$ se réduit à $2 \sum a^p b^p c^r$ et à $2.3 \sum a^p b^p c^p$, si en même temps r devient égal à p; on aura donc

$$\sum a^p b^p c^r = \frac{1}{2}\left(s_p^2 s_r - s_{2p}\, s_r - 2 s_{p+r}\, s_p + 2 s_{2p+r}\right)$$

et

$$\sum a^p b^p c^p = \frac{1}{6}\left(s_p^3 - 3 s_{2p}\, s_p + 2 s_{3p}\right).$$

En suivant la même marche, on calculera successivement les fonctions du quatrième ordre, puis celles du cinquième, et ainsi de suite; il est presque superflu d'ajouter que quand on aura calculé, en général, l'expression d'une fonction symétrique entière et homogène

du $n^{ième}$ ordre, si μ exposants deviennent égaux entre eux, il faudra diviser par $1.2.3...\mu$ la valeur qu'on aura trouvée.

On voit, par là, que toute fonction symétrique entière et homogène des racines d'une équation pourra s'exprimer rationnellement par les coefficients de cette équation, et que la même chose aura lieu, d'après les remarques faites à la leçon précédente, pour une fonction symétrique rationnelle quelconque.

Formation de l'équation d'où dépend une fonction rationnelle et non symétrique des racines d'une équation donnée.

Soient $a, b, c, \ldots, k, l$ les m racines d'une équation donnée $X = 0$, et

$$V = F(a, b, c, \ldots)$$

une fonction rationnelle donnée de ces racines, ou de quelques-unes d'entre elles. On pourra former l'équation en V, ainsi que nous l'avons vu dans la première leçon, en éliminant les quantités a, b, c, etc., entre l'équation précédente et les relations connues qui existent entre les coefficients et les racines de l'équation proposée; mais la méthode des fonctions symétriques fournit un moyen très-simple et beaucoup plus commode pour résoudre la même question. C'est la première application que nous ferons de cette théorie.

Si la fonction V contient n des m racines, le plus grand nombre de valeurs qu'elle puisse avoir en échangeant les lettres $a, b, c, \ldots, k, l$ les unes dans les autres de toutes les manières possibles, sera évidemment égal au nombre des arrangements de m lettres n à n, c'est-à-dire à

$$m(m-1)(m-2)\ldots(m-n+1).$$

Mais il peut arriver que le nombre des valeurs distinctes

de V soit beaucoup moindre; nous désignerons par μ ce nombre de valeurs, et par

$$V_1,\ V_2,\ V_3,\ \ldots,\ V_\mu$$

les μ valeurs de V. L'équation en V sera alors

$$(V-V_1)(V-V_2)\ldots(V-V_\mu)=0,$$

ou

$$V^\mu + P_1 V^{\mu-1} + P_2 V^{\mu-2} + \ldots + P_{\mu-1} V + P_\mu = 0,$$

en posant

$$\begin{aligned} V_1 + V_2 + \ldots + V_\mu &= -P_1,\\ V_1 V_2 + \ldots\ldots\ldots &= P_2,\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ V_1 V_2 \ldots V_\mu &= \pm P_\mu. \end{aligned}$$

Or les quantités $P_1, P_2, \ldots, P_\mu$ sont des fonctions symétriques des quantités V_1, V_2, etc.; et, par suite, elles sont aussi des fonctions symétriques des racines a, b, c, etc., de l'équation proposée : on pourra donc calculer les coefficients de l'équation en V par la méthode que nous avons exposée précédemment.

Nous avons admis comme évident que toute fonction symétrique des quantités V_1, V_2, etc. est aussi une fonction symétrique des racines a, b, c, etc. Voici, au surplus, un moyen très-facile de le démontrer.

Par hypothèse, les quantités

$$(1)\qquad V_1,\ V_2,\ \ldots,\ V_\mu$$

sont toutes distinctes, et ce sont les seules valeurs que V puisse avoir. Cela posé, faisons subir aux lettres

$$a,\ b,\ c,\ \ldots,\ k,\ l$$

une permutation quelconque, et supposons que V_1 se change en V'_1, V_2 en V'_2, etc.; les quantités

$$(2)\qquad V'_1,\ V'_2,\ \ldots,\ V'_\mu$$

devront toutes se trouver dans la série V_1, V_2, etc., puis-

que cette dernière comprend toutes les valeurs de V ; je dis, de plus, que tous les termes de la série (2) sont différents, et, par suite, sont les mêmes que ceux de la série (1) : on ne peut avoir, par exemple, $V'_1 = V'_2$, car V_1 et V_2 ne diffèrent de V'_1 et V'_2 qu'en ce que les quantités dont ces fonctions dépendent y sont désignées par des lettres différentes, et l'égalité $V'_1 = V'_2$ entraînerait, par conséquent, $V_1 = V_2$, ce qui est contre l'hypothèse. Il résulte de là que, si l'on fait subir aux lettres a, b, c, etc., un changement quelconque, les quantités V_1, V_2, etc., ne feront que s'échanger les unes dans les autres; par suite, une fonction symétrique de ces fonctions ne sera pas changée, et sera aussi symétrique par rapport aux quantités $a, b, c, \ldots, k, l$.

On peut dans bien des cas simplifier, par des artifices particuliers, le calcul de l'équation en V ; on en verra un exemple dans la recherche de l'équation qui a pour racines les carrés des différences des racines d'une équation donnée, prises deux à deux.

Équation aux carrés des différences.

Soient toujours $a, b, c, \ldots, k, l$ les m racines d'une équation $X = 0$, et posons

$$V = (a - b)^2;$$

l'équation en V sera du degré $\frac{m(m-1)}{2} = \mu$, qui est le nombre des combinaisons de m lettres deux à deux, puisque la fonction V est symétrique par rapport aux deux lettres qu'elle contient; et si l'on suppose que cette équation soit

$$V^\mu + P_1 V^{\mu-1} + P_2 V^{\mu-2} + \ldots = 0,$$

il suffira de calculer les quantités P_1, P_2, etc., qui sont des fonctions symétriques des racines de l'équation proposée : or ces coefficients P_1, P_2, etc., seront immédiate-

ment donnés par les formules de Newton, si l'on connaît les sommes des puissances semblables $S_1, S_2, \ldots, S_\mu$ des racines de l'équation en V. Tout est donc ramené à calculer ces dernières sommes en fonction des coefficients de l'équation proposée, ou en fonction des sommes s_1, s_2, etc., des puissances semblables de ses racines; puisque les sommes s_1, s_2, etc., s'expriment par les coefficients, à l'aide des formules de Newton.

Voici le procédé indiqué par Lagrange, pour calculer les sommes S_1, S_2, etc., relatives à l'équation en V, à l'aide des sommes s_1, s_2, etc., relatives à l'équation proposée.

Posons

$$\varphi(x) = (x-a)^{2n} + (x-b)^{2n} + \ldots + (x-l)^{2n};$$

en donnant à x successivement les valeurs $a, b, c, \ldots, k, l$, et ajoutant tous les résultats, on aura

$$\begin{aligned}\varphi(a) + \varphi(b) + \ldots + \varphi(l) = & (a-b)^{2n} + \ldots + (a-l)^{2n} \\ & + (b-a)^{2n} + \ldots + (b-l)^{2n} \\ & + \ldots\ldots\ldots\ldots\ldots\ldots \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & + (l-a)^{2n} + (l-b)^{2n} \ldots\ldots\end{aligned}$$

Or le second membre de cette équation est évidemment égal à $2S_n$; donc

$$2S_n = \varphi(a) + \varphi(b) + \ldots + \varphi(l).$$

D'un autre côté, en développant les différents termes de $\varphi(x)$, on trouve

$$\begin{aligned}\varphi(x) = & x^{2n} - 2nax^{2n-1} + \frac{2n(2n-1)}{1.2}a^2x^{2n-2} - \ldots + a^{2n} \\ & + x^{2n} - 2nbx^{2n-1} + \frac{2n(2n-1)}{1.2}b^2x^{2n-2} - \ldots + b^{2n} \\ & + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & + x^{2n} - 2nlx^{2n-1} + \frac{2n(2n-1)}{1.2}l^2x^{2n-2} - \ldots + l^{2n},\end{aligned}$$

ou

$$\varphi(x) = mx^{2n} - 2ns_1x^{2n-1} + \frac{2n(2n-1)}{1.2}s_2x^{2n-2} - \ldots + s_{2n}.$$

Remplaçant x successivement par $a, b, c, \ldots, l$, et ajoutant tous les résultats, on aura la valeur suivante de $\varphi(a) + \varphi(b) + \ldots + \varphi(l)$ ou de $2S_n$,

$$2S_n = ms_{2n} - 2ns_1s_{2n-1} + \frac{2n(2n-1)}{1.2}s_2s_{2n-2} - \ldots + ms_{2n}.$$

On voit aisément que les termes à égale distance des extrêmes sont égaux dans le second membre; par suite, on aura cette valeur de S_n,

$$S_n = ms_{2n} - 2ns_1s_{2n-1} + \frac{2n(2n-1)}{1.2}s_2s_{2n-2} - \ldots$$
$$\pm \frac{1}{2}\frac{2n(2n-1)\ldots(n+1)}{1.2.3\ldots n}s_ns_n.$$

En donnant à n les valeurs successives $1, 2, 3, \ldots, \mu$, on connaîtra les sommes $S_1, S_2, \ldots, S_\mu$ dont on a besoin; on achèvera ensuite le calcul, comme nous l'avons indiqué précédemment.

Cas de l'équation du troisième degré. — Prenons pour exemple l'équation du troisième degré

$$x^3 + px + q = 0.$$

On trouve

$$s_1 = 0, \quad s_2 = -2p, \quad s_3 = -3q,$$
$$s_4 = 2p^2, \quad s_5 = 5pq, \quad s_6 = 3q^2 - 2p^3;$$

ensuite

$$S_1 = 3s_2 - s_1^2 = -6p,$$
$$S_2 = 3s_4 - 4s_1s_3 + 3s_2^2 = 18p^2,$$
$$S_3 = 3s_6 - 6s_1s_5 + 15s_2s_4 - 10s_3^2 = -66p^3 - 81q^2,$$

et enfin

$$P_1 = 6p, \quad P_2 = 9p^2, \quad P_3 = 4p^3 + 27q^2.$$

L'équation aux carrés des différences des racines de $x^3+px+q=0$ est donc

$$V^3+6pV^2+9p^2V+(4p^3+27q^2)=0.$$

On suivrait une marche toute semblable pour former l'équation aux sommes deux à deux des racines d'une équation quelconque donnée.

La méthode générale dont nous venons de faire une application s'applique avec le même succès, que V soit une fonction entière ou non des racines a, b, c, etc.; mais on peut facilement démontrer que toute fonction rationnelle d'une ou plusieurs racines d'une équation peut toujours, si elle n'est pas entière, être remplacée par une fonction entière équivalente.

Sur la forme des fonctions rationnelles d'une ou plusieurs racines d'une équation.

Nous commencerons par établir le théorème suivant, relatif aux fonctions rationnelles d'une seule racine.

THÉORÈME. — *Toute fonction rationnelle et non entière d'une racine a d'une équation*

$$F(x)=0 \tag{1}$$

de degré m est équivalente à une fonction entière et de degré inférieur à m.

Soit, en effet, la fonction rationnelle $\frac{\varphi(a)}{\psi(a)}$, où φ et ψ désignent des fonctions entières; on aura identiquement

$$\frac{\varphi(a)}{\psi(a)}=\varphi(a)\cdot\frac{\psi(b)\psi(c)\ldots\psi(l)}{\psi(a)\cdot\psi(b)\ldots\psi(l)}, \tag{2}$$

$b, c, \ldots, l$ désignant les autres racines de l'équation (1). Or on voit que le dénominateur $\psi(a)\psi(b)\ldots\psi(l)$ du second membre est une fonction symétrique et entière des racines de l'équation (1), qui pourra, par conséquent, s'ex-

primer rationnellement par les coefficients connus de cette équation. Pareillement le facteur $\psi(b)\,\psi(c)\ldots\psi(l)$ du numérateur est une fonction symétrique et entière des racines de l'équation

$$\frac{F(x)}{x-a}=0,$$

et pourra s'exprimer sous forme rationnelle et entière, à l'aide des coefficients de cette équation, c'est-à-dire à l'aide de a et des coefficients de l'équation (1). D'après cela, l'égalité (2) prendra la forme

$$\frac{\varphi(a)}{\psi(a)}=\varphi(a).\theta(a),$$

où $\theta(a)$ désigne un polynôme entier et rationnel, par rapport à a. En effectuant le produit des polynômes φ et θ, notre fraction deviendra

$$\frac{\varphi(a)}{\psi(a)}=A_0+A_1a+A_2a^2+\ldots+A_\mu a^\mu;$$

et je dis qu'on peut supposer le degré μ inférieur à m. En effet, de l'équation $F(a)=0$ on peut tirer la valeur de a^m qui sera exprimée par un polynôme de degré $m-1$; en multipliant par a cette valeur de a^m, on aura a^{m+1} qui sera exprimé par un polynôme du degré m, mais qu'on pourra abaisser au degré $m-1$, en remplaçant a^m par sa valeur trouvée précédemment. En continuant ainsi, on exprimera toutes les puissances de a, à partir de la $m^{\text{ième}}$, à l'aide de polynômes de degré $m-1$, et, par suite, on pourra chasser de l'expression de $\frac{\varphi(a)}{\psi(a)}$ que nous avons trouvée, toutes les puissances de a supérieures à la $(m-1)^{\text{ième}}$. Mais on peut aussi opérer comme il suit : Si μ est $>m$, on divisera le polynôme $A_0+A_1a+\ldots$ par $F(a)$, et en désignant par Q le quotient et par $\varpi(a)$ le

reste qui est de degré inférieur à m, on aura

$$\frac{\varphi(a)}{\psi(a)} = A_0 + A_1 a + \ldots = F(a) \times Q + \varpi(a);$$

et comme $F(a)$ est nul, on aura simplement

$$\frac{\varphi(a)}{\psi(a)} = \varpi(a),$$

où ϖ désigne un polynôme de degré $m - 1$ au plus.

Quoique la démonstration précédente ne laisse rien à désirer sous le rapport de la rigueur et de la clarté, nous en donnerons une seconde qui aura l'avantage de nous fournir un procédé plus facile pour trouver la forme entière qui convient à une fonction fractionnaire donnée.

Soit toujours $\frac{\varphi(a)}{\psi(a)}$ la fraction donnée, où a est racine de $F(x) = 0$. On peut supposer $\psi(a)$ de degré inférieur à m; car si le contraire avait lieu, on ferait disparaître de $\psi(a)$ les puissances de a supérieures à la $(m-1)^{\text{ième}}$ par l'un des procédés indiqués précédemment.

Cela posé, opérons sur les polynômes $F(a)$ et $\psi(a)$, comme s'il était question de trouver leur plus grand commun diviseur; on aura cette suite d'égalités :

$$\begin{aligned}
F(a) &= \psi(a)\,Q_1 + R_1, \\
\psi(a) &= R_1 Q_2 + R_2, \\
R_1 &= R_2 Q_3 + R_3, \\
&\ldots\ldots\ldots\ldots \\
R_{n-2} &= R_{n-1} Q_n + R_n,
\end{aligned}$$

où R_n ne contient plus la quantité a. Or, $F(a)$ étant nul, on aura

$$\begin{aligned}
R_1 &= -\,Q_1\,\psi(a), \\
R_2 &= (1 + Q_1 Q_2)\,\psi(a), \\
R_3 &= -\,(Q_1 + Q_3 + Q_1 Q_2 Q_3)\,\psi(a), \\
&\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

La dernière de ces égalités sera de la forme

$$R_n = \theta(a).\psi(a),$$

$\theta(a)$ désignant un polynôme entier et rationnel par rapport à a. On en tire

$$\psi(a) = \frac{R_n}{\theta(a)},$$

et, par suite,

$$\frac{\varphi(a)}{\psi(a)} = \frac{\varphi(a).\theta(a)}{R_n}.$$

Cette valeur de $\frac{\varphi(a)}{\psi(a)}$ est entière par rapport à a, puisque R_n ne contient pas a; et, si elle contient des puissances de a supérieures à la $(m-1)^{ième}$, on pourra les faire disparaître par le procédé que nous avons indiqué précédemment.

A la vérité, cette méthode semble en défaut dans le cas où les polynômes $\psi(x)$ et $F(x)$ ont un diviseur commun; car, dans ce cas, la quantité désignée par R_n est nulle, ainsi que $\theta(a)$: mais alors on pourra enlever de $F(x)$, par une simple division, tous les facteurs linéaires qui sont dans $\psi(x)$, et parmi lesquels ne se trouve pas $x-a$, car autrement $\psi(a)$ serait nul. En désignant par $F_1(x)$ le résultat ainsi obtenu, a sera racine de $F_1(x)=0$, et le polynôme $\psi(x)$ étant dès lors premier avec $F_1(x)$, on pourra appliquer la méthode précédente.

Corollaire. — La fonction rationnelle la plus générale d'une racine d'une équation de degré m est une fonction entière du degré $m-1$, renfermant par conséquent m coefficients arbitraires.

Extension aux fonctions rationnelles de plusieurs racines d'une équation. — La méthode précédente a surtout l'avantage de pouvoir être appliquée aux fonctions rationnelles de plusieurs racines d'une équation. On a,

en effet, ce théorème : *Toute fonction rationnelle non entière de plusieurs racines d'une équation peut être remplacée par une fonction entière des mêmes racines.*

Rien ne sera changé à nos raisonnements, si la fonction $\frac{\varphi(a)}{\psi(a)}$, que nous avons considérée, renferme d'autres racines b, c, etc., de l'équation $F(x) = 0$, et cette fonction pourra se mettre sous la forme $A_0 a + A_1 a^2 + \ldots$, A_0 et A_1 étant des fonctions rationnelles de racines parmi lesquelles ne se trouve pas a. A leur tour, on pourra rendre ces fonctions A_0, A_1, etc., entières par rapport à une autre racine b, puis par rapport à une troisième, et ainsi de suite.

Exemple. — Toute fonction rationnelle d'une racine a de l'équation du troisième degré

$$x^3 + px^2 + qx + r = 0$$

pourra être mise sous la forme

$$A + Ba + Ca^2;$$

mais il est souvent préférable de prendre une forme fractionnaire dont les deux termes soient linéaires, et cela est toujours possible; car, si l'on divise les polynômes $a^3 + pa^2 + qa + r$ et $A + Ba + Ca^2$, dont le premier est nul, l'un par l'autre, on aura un quotient et un reste du premier degré en a, et l'on en conclura aisément que la fonction $A + Ba + Ca^2$ peut être mise sous la forme $\frac{Ma + N}{a + P}$.

TROISIÈME LEÇON.

Méthode de M. Cauchy pour calculer une fonction symétrique rationnelle et entière des racines d'une équation. — Méthode d'élimination fondée sur la théorie des fonctions symétriques. — Théorème sur le degré de l'équation finale résultant de l'élimination d'une inconnue entre deux équations qui en contiennent plusieurs.

Méthode de M. Cauchy.

M. Cauchy a publié, dans ses anciens *Exercices de Mathématiques* (4ᵉ année), une méthode fort élégante pour trouver la valeur d'une fonction symétrique et entière des racines d'une équation. Cette méthode consiste à éliminer successivement de l'expression de la fonction symétrique qu'on veut évaluer, chacune des racines de l'équation proposée; elle repose sur la proposition suivante :

Soit V une fonction symétrique et entière des racines $a, b, c, \ldots, i, k, l$ d'une équation

$$x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0,$$

que nous représenterons aussi, pour abréger, par

$$X = 0;$$

et supposons qu'ayant éliminé de l'expression de V, par un moyen quelconque, toutes les racines excepté a, on ait mis la valeur de cette fonction sous la forme d'un polynôme entier et rationnel ordonné par rapport aux puissances de a, que l'on ait, par exemple,

$$V = A_0 a^{\mu} + A_1 a^{\mu-1} + \ldots + A_{\mu-1} a + A_{\mu},$$

A_0, A_1, etc., étant des quantités composées rationnelle-

ment avec les coefficients de l'équation proposée; je dis que si l'on divise cette expression de V par le polynôme

$$A = a^m + p_1 a^{m-1} + p_2 a^{m-2} + \ldots + p_{m-1} a + p_m,$$

obtenu en remplaçant x par a dans X, le reste de la division sera indépendant de a, et sera précisément la valeur de la fonction V.

En effet, si Q et R désignent le quotient et le reste de la division V par A, on aura $V = AQ + R$, et comme A est nul,

$$V = R.$$

D'ailleurs, ce reste R est au plus du degré $m-1$ en a; nous le représenterons par

$$q_0 a^{m-1} + q_1 a^{m-2} + \ldots + q_{m-2} a + q_{m-1},$$

et l'on aura

$$V = q_0 a^{m-1} + q_1 a^{m-2} + \ldots + q_{m-2} a + q_{m-1}.$$

Mais V étant une fonction symétrique, on peut changer a et b l'un dans l'autre, ainsi que a et c, etc.; et, comme par ces changements, q_0, q_1, etc., conservent leurs valeurs, il s'ensuit que l'équation

$$q_0 x^{m-1} + q_1 x^{m-2} + \ldots + q_{m-2} x + (q_{m-1} - V) = 0$$

sera satisfaite en remplaçant x par l'une quelconque des m racines $a, b, \ldots, k, l$; ce qui est impossible, à moins que les coefficients ne soient tous nuls, puisque cette équation n'est que du degré $m-1$: on aura donc, en particulier $q_{m-1} - V = 0$, ou

$$V = q_{m-1},$$

comme nous l'avions annoncé.

La démonstration précédente suppose que les m racines $a, b, c, \ldots, k, l$ sont toutes inégales; mais les conclusions précédentes ne subsistent pas moins, si quelques-unes de ces racines sont égales entre elles. Nous emploie-

rons, pour justifier cette assertion, un raisonnement dont on fait un fréquent usage en analyse.

Si l'équation $X = 0$ a des racines égales, on considérera d'abord à sa place une équation $X_1 = 0$, dont toutes les racines seront inégales, et qu'on obtiendra en faisant subir des modifications insensibles aux coefficients de $X = 0$; par exemple, si X a trois racines égales à a, et que toutes les autres soient différentes, on prendra

$$X_1 = \frac{X(x-a-h)(x-a-h')}{(x-a)^2}.$$

Le polynôme X_1 ne diffère de X qu'en ce que deux des trois racines égales à a sont remplacées par $a+h$ et $a+h'$: on voit aisément, sans qu'il soit nécessaire d'insister davantage, comment on devrait choisir le polynôme X_1, si, outre les trois racines égales à a, l'équation proposée avait plusieurs racines égales à b, à c, etc. Cela posé, substituant l'équation $X_1 = 0$ à $X = 0$, et conservant d'ailleurs les notations précédentes, on arrivera à l'équation

$$V = q_{m-1},$$

et cette équation aura lieu, quelque petites que soient les quantités h, h', etc.; elle aura donc lieu aussi à la limite, c'est-à-dire quand on fera $h = 0$, $h' = 0$, etc.

Voici maintenant quelle est la méthode indiquée par M. Cauchy, pour calculer la valeur d'une fonction V symétrique et entière des racines $a, b, c, \ldots, i, k, l$ de l'équation

$$X = x^m + p_1 x^{m-1} + p_2 x^{m-2} + p_m = 0.$$

Divisons X par $x - a$, et désignons par X_1 le quotient; divisons de même X_1 par $x - b$, et désignons par X_2 le quotient, puis X_2 par $x - c$, et soit X_3 le quotient, et continuons ainsi d'enlever de X tous les facteurs linéaires jusqu'à $x - k$ inclusivement, en sorte que

X_{m-1} ne contiendra plus que le seul facteur $x - l$. Cela posé, considérons les m équations

$$X = 0, \quad X_1 = 0, \quad X_2 = 0, \ldots, X_{m-1} = 0.$$

La première n'est autre que la proposée, et a pour racines $a, b, c, \ldots, k, l$; la seconde a pour racines $b, c, \ldots, k, l$, et ses coefficients sont exprimés sous forme entière à l'aide de a et des coefficients de la proposée; la troisième a pour racines $c, \ldots, k, l$, et ses coefficients sont exprimés sous forme entière à l'aide de b et des coefficients de la précédente, c'est-à-dire à l'aide de a, b et des coefficients de la proposée; et, en général, les coefficients de l'une quelconque de ces équations sont exprimés sous forme entière à l'aide des coefficients et des racines de la proposée qui n'appartiennent pas à l'équation que l'on considère; enfin, désignons par A la valeur de X pour $x = a$, par B la valeur de X_1 pour $x = b$, par C celle de X_2 pour $x = c$, et ainsi de suite, en sorte que I sera la valeur de X_{m-3} pour $x = i$, K celle de X_{m-2} pour $x = k$, et enfin L celle de X_{m-1} pour $x = l$; on aura

$$A = 0, \quad B = 0, \quad C = 0, \ldots, I = 0, \quad K = 0, \quad L = 0.$$

Cela posé, V est une fonction symétrique, non-seulement des racines de l'équation $X = 0$, mais aussi de celles de l'une quelconque des équations

$$X = 0, \quad X_1 = 0, \ldots, X_{m-3} = 0, \quad X_{m-2} = 0, \quad X_{m-1} = 0.$$

Nous allons faire voir comment, en s'appuyant sur cette remarque, on peut, à l'aide du théorème fondamental démontré au commencement de cette leçon, éliminer successivement chaque racine de l'expression de V.

D'abord l'équation $L = 0$, où l entre au premier degré, permet de chasser immédiatement l de l'expression de V. Considérant alors V comme fonction symétrique des

deux racines k et l de l'équation $X_{m-2} = 0$, dont l'une l est déjà éliminée, on l'ordonnera par rapport à k, et on la divisera par K, conformément à ce qui a été dit plus haut; le reste de la division ne contiendra pas k et sera la valeur de V débarrassée des racines k et l. On considérera alors V comme fonction symétrique des trois racines i, k, l de l'équation $X_{m-3} = 0$, dont les deux dernières n'entrent plus dans son expression, et l'ayant ordonnée par rapport à i, on la divisera par I à l'effet d'éliminer i; le reste de la division ne contiendra pas i et sera la valeur de V débarrassée des trois racines i, k, l. On continuera de la même manière, jusqu'à ce qu'on ait éliminé de V chacune des racines $a, b, c, \ldots, i, k, l$; on aura alors la valeur de cette fonction exprimée par les coefficients de l'équation proposée.

Il importe de remarquer que l'expression définitive de V s'obtient par de simples divisions, et que les premiers termes des polynômes A, B, C, ..., I, K, L, qui servent successivement de diviseurs, ont tous l'unité pour coefficient : par conséquent, ces divisions n'introduiront aucun dénominateur; en sorte que si l'expression primitive de V est entière, non-seulement par rapport aux racines $a, b, c, \ldots, i, k, l$, qui y entrent symétriquement, mais aussi par rapport aux coefficients p_1, p_2, etc., qui peuvent aussi y entrer, l'expression définitive de V sera aussi entière par rapport à ces coefficients, et enfin, si ces coefficients sont des nombres entiers, V sera lui-même un nombre entier. Ce théorème important, que nous n'avions pas établi complétement par la méthode exposée dans la leçon précédente, se déduit immédiatement, comme on vient de voir, de la méthode de M. Cauchy.

Application à un exemple. Détermination du dernier terme de l'équation aux carrés des différences. — Je choisis cet exemple, pour montrer comment on peut,

par des artifices convenables, simplifier dans certains cas l'emploi de la méthode de M. Cauchy. Nous supposerons que l'on sache former le dernier terme de l'équation aux carrés des différences pour une équation du degré $m-1$, et nous allons chercher à en déduire la valeur de la même fonction pour une équation de degré m. Soient toujours $a, b, c, \ldots, k, l$ les m racines de l'équation

$$(1)\qquad X = x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} + p_m = 0;$$

soient aussi

$$V = (a-b)^2 (a-c)^2 \ldots \ldots \ldots \ldots (k-l)^2$$

et

$$V_1 = (b-c)^2 (b-d)^2 \ldots \ldots \ldots \ldots (k-l)^2;$$

V sera le dernier terme de l'équation aux carrés des différences des racines de l'équation (1), et V_1 le dernier terme de l'équation aux carrés des différences des racines de l'équation

$$\frac{X}{x-a} = 0,$$

ou

$$(2)\qquad \begin{array}{l|l|l} x^{m-1} + p_1 & x^{m-2} + p_2 & x^{m-3} + \ldots + a^{m-1} = 0, \\ \quad\;\; + a & \qquad\;\; + p_1 a & \qquad\qquad\;\; + p_1 a^{m-2} \\ & \qquad\;\; + a^2. & \qquad\qquad\;\; + \ldots\ldots\ldots \\ & & \qquad\qquad\;\; \ldots\ldots\ldots\ldots \\ & & \qquad\qquad\;\; + p^{m-1}. \end{array}$$

Cela posé, on a

$$V = V_1 (a-b)^2 (a-c)^2 \ldots (a-k)(a-l)^2.$$

Or le produit $(a-b)(a-c)\ldots(a-k)(a-l)$ est, comme on sait, égal à la valeur que prend la dérivée du polynôme X pour $x=a$, c'est-à-dire à

$$m a^{m-1} + (m-1) p_1 a^{m-2} + \ldots + p_{m-1};$$

donc on aura

$$V = V_1 [m a^{m-1} + (m-1) p_1 a^{m-2} + \ldots + p_{m-1}]^2.$$

D'ailleurs, nous admettons qu'on sache exprimer la valeur de V_1 par les coefficients de l'équation (2), c'est-à-dire en fonction de a et des coefficients de la proposée; donc la fonction V pourra elle-même être mise sous la forme d'un polynôme ordonné par rapport aux puissances de a, et, en divisant ce polynôme par le premier membre de l'équation proposée, dans lequel on aura remplacé x par a, le reste de la division donnera la valeur cherchée de V.

Cela posé, on sait calculer la fonction V pour une équation du second degré; on pourra donc calculer cette fonction pour l'équation du troisième degré, puis pour celle du quatrième, et ainsi de suite.

Cas du troisième degré. — L'équation proposée sera

$$x^3 + px^2 + qx + r = 0,$$

et l'on aura

$$V = (a-b)^2(a-c)^2(b-c)^2,$$
$$V_1 = (b-c)^2,$$
$$V = V_1(a-b)^2(a-c)^2;$$

V_1 étant relatif à l'équation du deuxième degré

$$\begin{array}{l|l} x^2 + p & x + q = 0, \\ \quad\; + a & \;\; + pa \\ & \;\; + a^2 \end{array}$$

on a immédiatement

$$V_1 = (p+a)^2 - 4(q + pa + a^2) = -3a^2 - 2pa + (p^2 - 4q);$$

d'ailleurs

$$(a-b)(a-c) = 3a^2 + 2pa + q,$$

par suite,

$$\begin{array}{l} V = (-3a^2 - 2pa + p^2 - 4q)(3a^2 + 2pa + q)^2 \\ \quad = -27a^6 - 54pa^5 \begin{array}{l|l|l|l|l} -27p^2 & a^4 + 4p^3 & a^3 + 4p^4 & a^2 + 4p^3q & a + p^2q^2. \\ -54q & \quad -72pq & \quad -18p^2q & \quad -18pq^2 & \quad -4q^3 \\ & & \quad -27q^2 & & \end{array} \end{array}$$

Divisant cette valeur de V par $a^3 + pa^2 + qa + r$, on

trouve pour quotient

$$-27a^3-27pa^2-27qa+(4p^3+27r-18pq),$$

et pour reste,

$$-4q^3-27r^2+18pqr+p^2q^2-4p^3r,$$

ce qui est précisément la valeur de V que nous cherchons.

Méthode d'élimination fondée sur la théorie des fonctions symétriques.

Parmi les applications que l'on peut faire de la théorie des fonctions symétriques, l'une des plus importantes est, sans contredit, la méthode d'élimination que nous allons expliquer.

Considérons deux équations, des degrés m et n respectivement, contenant deux ou un plus grand nombre de variables x, y, etc., et entre lesquelles il s'agit d'éliminer x. Nous supposerons ces équations complètes, et leurs coefficients entièrement indéterminés, et les ordonnant par rapport à x, nous les représenterons par

$$(1)\quad x^m+p_1x^{m-1}+p_2x^{m-2}+\ldots+p_{m-1}x+p_m=0,$$

$$(2)\quad x^n+q_1x^{n-1}+q_2x^{n-2}+\ldots+q_{n-1}x+q_n=0.$$

Les coefficients p_1, p_2, etc., q_1, q_2, etc., sont des fonctions entières de y, etc.

Désignons par $a, b, c, \ldots, k, l$ les m racines de la première de ces deux équations, lesquelles dépendent de y et des autres variables, s'il y en a, et portons-les dans la seconde; on aura ces m résultats

$$(3)\quad \left\{\begin{array}{l} a^n+q_1a^{n-1}+q_2a^{n-2}+\ldots+q_{n-1}a+q_n,\\ b^n+q_1b^{n-1}+q_2b^{n-2}+\ldots+q_{n-1}b+q_n,\\ c^n+q_1c^{n-1}+q_2c^{n-2}+\ldots+q_{n-1}c+q_n,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ l^n+q_1l^{n-1}+q_2l^{n-2}+\ldots+q_{n-1}l+q_n. \end{array}\right.$$

Cela posé, si l'on multiplie ensemble tous ces résultats, et que l'on désigne par V leur produit, il est facile de voir que

$$V = 0$$

sera l'équation finale résultant de l'élimination de x entre les deux équations proposées. En effet, l'équation finale résultant de l'élimination de x entre deux équations est simplement la condition nécessaire pour que ces deux équations aient une racine commune, et il est bien évident que la condition nécessaire et suffisante pour que les équations (1) et (2) aient une racine commune, est que l'un des résultats (3), ou leur produit V, soit nul.

D'ailleurs, V est une fonction symétrique et entière des racines de l'équation (1), qui contient en outre rationnellement les coefficients de l'équation (2); on pourra donc exprimer cette fonction rationnellement à l'aide des coefficients des équations (1) et (2).

L'application de la méthode précédente à deux équations, dont les coefficients ont des valeurs particulières, conduit toujours à la véritable équation finale, pourvu que ces équations contiennent la plus haute puissance de l'inconnue qu'on élimine. Cette méthode a, en outre, l'avantage de conduire à un théorème important, dont nous allons présenter la démonstration.

Théorème sur le degré de l'équation finale, résultant de l'élimination d'une inconnue entre deux équations.

Nous conserverons les notations employées dans le précédent paragraphe, et nous supposerons toujours que les deux équations (1) et (2), l'une du degré m, l'autre du degré n, soient complètes, et que leurs coefficients, représentés chacun par une lettre, soient dans une parfaite indépendance. Alors les quantités p_1 et q_1 sont des fonctions entières

du premier degré par rapport aux variables y, etc., qui entrent dans les équations proposées; pareillement, p_2, q_2 seront du second degré, et, en général, le degré des coefficients de x dans les équations (1) et (2) sera indiqué par leur indice. Cela posé, nous allons démontrer le théorème suivant.

Le degré de l'équation finale résultant de l'élimination d'une variable x entre deux équations complètes dont les coefficients sont indéterminés et indépendants les uns des autres, est précisément égal au produit des degrés des deux équations.

Considérons, en effet, un terme quelconque du produit des expressions (3), par exemple

$$q_{n-\alpha}\, q_{n-6} \ldots q_{n-\lambda}\, a^{\alpha}\, b^{6} \ldots l^{\lambda};$$

ce terme se trouvera dans V, ainsi que la fonction symétrique dont il fait partie. V est donc la somme d'expressions de la forme

$$q_{n-\alpha}\, q_{n-6} \ldots q_{n-\lambda} \sum a^{\alpha}\, b^{6} \ldots l^{\lambda},$$

en observant qu'il faut remplacer $q_{n-\alpha}$ par 1, si $\alpha = n$, et de même pour les autres. Or, d'après ce qui a été dit plus haut, le facteur $q_{n-\alpha}\, q_{n-6} \ldots q_{n-\lambda}$ est du degré $(n-\alpha)+(n-6)+\ldots+(n-\lambda)$ ou $mn-(\alpha+6+\ldots+\lambda)$ par rapport aux variables y, etc.; si donc nous faisons voir que le second facteur $\sum a^{\alpha}\, b^{6} \ldots l^{\lambda}$ est, par rapport à ces mêmes variables y, etc., du degré $\alpha+6+\ldots+\lambda$, il s'ensuivra que le terme de V que nous considérons est du degré mn, et que V est lui-même de ce degré. Les coefficients p_1, p_2, etc., de l'équation (1) étant, par rapport à y, etc., d'un degré égal à leur indice, il en sera de même des sommes de puissances semblables s_1, s_2, etc., de ses racines; cela résulte immédiatement des

formules de Newton. Ainsi, le degré d'une fonction symétrique simple telle que s_α est le même, soit que l'on considère s_α comme fonction de a, b, etc., soit qu'on la considère comme fonction de y, etc. Enfin, $\sum a^\alpha b^6 \ldots l^\lambda$ peut s'exprimer à l'aide des sommes s_α par une formule entière qui sera du degré $\alpha + 6 + \ldots + \lambda$ par rapport aux racines a, b, etc., et qui sera, par conséquent, aussi du même degré par rapport à y, etc. Le théorème est donc démontré.

Nous avons admis comme évident que les termes de degré mn, qui se trouvent dans V, ne peuvent se détruire, tant qu'on laisse indéterminés les coefficients des équations (1) et (2). Voici, au surplus, un moyen très-simple de le démontrer.

Considérons les deux équations

$$(1') \quad (x + a_1 y + b_1)(x + a_2 y + b_2)\ldots(x + a_m y + b_m) = 0,$$
$$(2') \quad (x + c_1 y + d_1)(x + c_2 y + d_2)\ldots(x + c_n y + d_n) = 0,$$

entre les deux inconnues x et y, et qui ont pour premiers membres, l'une (1') un produit de m facteurs linéaires, l'autre (2') un produit de n facteurs pareillement linéaires.

L'équation finale résultant de l'élimination de x entre les deux équations (1') et (2') aura évidemment pour premier membre le produit des mn facteurs linéaires dont l'expression générale est

$$(a_\mu - c_\nu) y + (b_\mu - d_\nu),$$

μ et ν pouvant prendre toutes les valeurs de 1 à m et de 1 à n respectivement; et si on laisse indéterminées les quantités $a_1, b_1, c_1, d_1, \ldots$, cette équation finale sera du degré mn.

D'ailleurs, cette équation finale doit être comprise dans l'équation $V = 0$, qui est relative aux équations géné-

rales (1) et (2); donc cette dernière ne saurait être d'un degré inférieur à mn, à moins qu'on ne suppose aux coefficients des valeurs particulières.

Si les coefficients des équations (1) et (2) ont des valeurs déterminées, on pourra toujours appliquer le raisonnement qui précède, pourvu que ces équations contiennent la plus haute puissance de l'inconnue qu'on élimine. On est alors conduit à la proposition suivante, qui est générale.

Le degré de l'équation finale résultant de l'élimination d'une inconnue entre deux équations qui en contiennent plusieurs, est au plus égal au produit des degrés de ces équations.

Ce théorème a lieu encore, si les équations que l'on considère manquent de la plus haute puissance de l'inconnue qu'on élimine.

Soient, en effet, deux équations entre deux variables x et y, ayant respectivement m et n pour degrés et manquant du terme le plus élevé en x. En considérant x et y comme des coordonnées rectilignes, ces deux équations appartiendront à deux courbes, et le degré de l'équation finale résultant de l'élimination de y sera le nombre des points d'intersection réels ou imaginaires de ces courbes. Par conséquent, ce nombre ne changera évidemment pas, si l'on rapporte les deux courbes à d'autres axes de coordonnées; mais alors les nouvelles équations de ces deux courbes se déduisent des anciennes, en remplaçant x et y par des fonctions linéaires $ax+by$, $a'x+b'y$, et contiendront évidemment, l'une un terme en x^m, l'autre un terme en x^n, à cause de l'indétermination de a et a'; le degré de l'équation finale en y résultant de l'élimination de x entre ces nouvelles équations sera donc au plus égal à mn : par suite, le nombre des points d'intersection des deux courbes ne pourra surpasser mn, et il en

sera de même du degré de l'équation finale résultant de l'élimination de y entre les deux proposées.

La même chose aura lieu si les deux équations proposées contiennent, outre x et y, d'autres variables u, z, ... En effet, si l'on pose

$$z = ky, \quad u = k'y, \ldots,$$

et que l'on considère k, k', ..., comme des paramètres, le raisonnement précédent s'appliquera aux deux équations proposées, qui ne renferment plus que x et y. Par où l'on voit que l'équation finale en y, z, u, ..., résultant de l'élimination de x, sera au plus du degré mn, si l'on y remplace z, u, ..., par ky, $k'y$..., et cela, quels que soient k, k',...; mais cette substitution ne change évidemment pas son degré, lequel ne pourra donc, en aucun cas, surpasser mn.

La méthode d'élimination par les fonctions symétriques, telle que nous l'avons exposée, ne donne pas le moyen de déterminer, dans la résolution de deux équations simultanées, la valeur de la seconde inconnue, qu'il faut joindre à chaque racine de l'équation finale. M. Liouville a cherché à combler cette lacune, et il y est parvenu (tome XII du *Journal de Mathématiques pures et appliquées*), comme nous l'indiquerons dans la leçon suivante.

QUATRIÈME LEÇON.

Méthode de M. Liouville pour la résolution de deux équations à deux inconnues, en employant la méthode d'élimination par les fonctions symétriques, et en supposant connues les racines de l'équation finale. — Extension au cas d'un nombre quelconque d'équations entre un même nombre d'inconnues. — Méthode d'Abel pour déterminer la racine commune à deux équations. — Théorème de Lagrange sur les conditions nécessaires pour que deux équations aient plusieurs racines communes.

Méthode de M. Liouville pour la résolution de deux équations à deux inconnues.

Soient deux équations

(1) $$f(x, y) = 0, \quad F(x, y) = 0,$$

entre deux inconnues x et y; nous introduirons une autre variable t, telle que l'on ait

(2) $$t = x + \alpha y \quad \text{ou} \quad x = t - \alpha y,$$

α désignant un *paramètre* indéterminé. En mettant, au lieu de x, sa valeur $t - \alpha y$, les équations proposées deviennent

(3) $$f(t - \alpha y, y) = 0, \quad F(t - \alpha y, y) = 0.$$

Cela posé, nous éliminerons y, entre les équations (3), par un moyen quelconque; nous obtiendrons ainsi une équation finale en t, renfermant le paramètre α, et nous la représenterons par

(4) $$\psi(t, \alpha) = 0;$$

comme pour $\alpha = 0$, on a $t = x$, l'équation finale en x

qui résulterait de l'élimination de y entre les équations (1) sera d'abord

$$\psi(x, o) = o. \tag{5}$$

Voici maintenant comment on obtiendra la valeur de y qui correspond à chaque racine x de cette équation finale. Considérons t et α comme des coordonnées rectangulaires; l'équation (4) appartiendra à un lieu qui n'est autre chose qu'un système de droites réelles ou imaginaires, lesquelles seront aussi représentées par l'équation linéaire

$$t = x + \alpha y,$$

où l'on doit remplacer x et y successivement par les divers couples de solutions communes aux équations (1).

Considérons, en particulier, un couple de valeurs de x et y satisfaisant aux proposées, et la droite correspondante $t = x + \alpha y$, dont l'ordonnée à l'origine est $OM = x$ (*fig.* 1), et le coefficient angulaire tang $MAO = y$.

Cela posé, supposons d'abord qu'à la valeur x que nous considérons ne corresponde qu'une seule valeur de y; la droite AB sera la seule des droites représentées par l'équation (4), qui passera par le point M : en d'autres termes, la droite AB sera la seule tangente au point M du lieu que représente l'équation (4). Mais le coefficient angulaire de la tangente en un point quelconque (t, α) de ce lieu s'obtient en différentiant l'équation (4); ce qui donne

$$\frac{d\psi}{d\alpha} + \frac{d\psi}{dt}\frac{dt}{d\alpha} = o, \tag{6}$$

d'où

$$\frac{dt}{d\alpha} = -\frac{\dfrac{d\psi}{d\alpha}}{\dfrac{d\psi}{dt}} = \psi_1(t, \alpha),$$

équation qui ne sera en défaut que si l'on a en même

temps $\frac{d\psi}{d\alpha} = 0$, $\frac{d\psi}{dt} = 0$; ce qui n'a lieu que pour les points singuliers. Nous savons, d'ailleurs, qu'au point M, qui a pour coordonnées $\alpha = 0$ et $t = x$, la tangente a pour coefficient angulaire y; on aura donc

$$y = \psi_1(x, 0),$$

et notre problème est résolu.

L'application de cette méthode exige un calcul plus long que si l'on se proposait seulement l'élimination de y entre les deux équations proposées; car le premier membre de l'équation finale (5) n'est que le premier terme de l'équation (4) ordonnée par rapport à α : mais on peut démontrer facilement qu'il n'est pas nécessaire de calculer l'équation (4) tout entière, et qu'il suffit d'en connaître les deux premiers termes. Imaginons, en effet, que le polynôme $\psi(t, \alpha)$ soit ordonné par rapport aux puissances de α, de sorte que l'on ait

$$(7) \qquad \psi(t, \alpha) = \varpi(t) + \alpha\varpi_1(t) + \alpha^2\varpi_2(t) + \ldots,$$

et qu'on connaisse les deux premiers termes $\varpi(t)$ et $\varpi_1(t)$; l'équation finale en x sera d'abord

$$\varpi(x) = 0.$$

Ensuite on tire, en différentiant l'équation (7), et dénotant les dérivées à la manière de Lagrange,

$$(8) \quad \begin{cases} \frac{d\psi}{dt} = \varpi'(t) + \alpha\varpi_1'(t) + \ldots, \\ \frac{d\psi}{d\alpha} = \varpi_1(t) + 2\alpha\varpi_2(t) + \ldots; \end{cases}$$

d'où

$$\psi_1(t, \alpha) = -\frac{\varpi_1(t) + 2\alpha\varpi_2(t) + \ldots}{\varpi'(t) + \alpha\varpi_1'(t) + \ldots},$$

et, par conséquent,

$$y = -\frac{\varpi_1(x)}{\varpi'(x)}.$$

L'équation précédente fera connaître la valeur de y qui correspond à chaque racine x, et elle ne sera en défaut que pour les valeurs de x auxquelles correspondent plusieurs valeurs de y. C'est le cas que nous allons actuellement examiner.

Supposons qu'à une même racine x de l'équation (5) correspondent deux valeurs de y que nous désignerons par y et y_1; alors les droites AB, A_1B_1 (*fig.* 2), représentées par les équations

$$t = x + \alpha y, \quad t = x + \alpha y_1,$$

passeront par un même point M de l'axe OT: autrement dit, au point M, qui est un point de la ligne représentée par l'équation (4); il y a deux tangentes à cette ligne, AB et A_1B_1; on a donc en ce point $\frac{d\psi}{d\alpha} = 0$, $\frac{d\psi}{dt} = 0$, et pour avoir la valeur de $\frac{dt}{d\alpha}$, il faut différentier l'équation (6), ce qui donne, à cause de $\frac{d\psi}{dt} = 0$,

$$\frac{d^2\psi}{d\alpha^2} + 2\frac{d^2\psi}{d\alpha\, dt}\frac{dt}{d\alpha} + \frac{d^2\psi}{dt^2}\left(\frac{dt}{d\alpha}\right)^2 = 0. \tag{9}$$

En faisant $\alpha = 0$ et $t = x$, on tirera de cette équation deux valeurs de $\frac{dt}{d\alpha}$, qui seront précisément celles de y et y_1; et l'on peut voir aisément qu'il suffit de connaître les trois premiers termes de $\psi(t, \alpha)$. Différentions, en effet, les équations (8); on aura

$$\frac{d^2\psi}{dt^2} = \varpi''(t) + \alpha\varpi_1''(t) + \ldots,$$

$$\frac{d^2\psi}{d\alpha\, dt} = \varpi_1'(t) + 2\alpha\varpi_2'(t) + \ldots,$$

$$\frac{d^2\psi}{d\alpha^2} = 2\varpi_2(t) + \ldots.$$

D'après cela, faisant dans l'équation (9), $\alpha = 0$, $t = x$,

$\frac{dt}{dx} = y$, on aura

$$\varpi''(x) y^2 + 2\varpi'_1(x) y + 2\varpi_2(x) = 0,$$

équation qui a pour racines les deux valeurs y et y_1, qui correspondent à x.

On voit, par là, comment il faudra opérer, si à une même valeur de x correspondent trois ou un plus grand nombre de valeurs de y. Je ne pense pas qu'il soit nécessaire d'insister davantage. Remarquons seulement que, pour qu'à une valeur de x correspondent deux valeurs de y, il faut que l'on ait en même temps

$$\varpi'(x) = 0, \quad \varpi_1(x) = 0;$$

pour qu'il y ait trois valeurs de y correspondantes à la valeur de x, il faut, de plus, que l'on ait

$$\varpi''(x) = 0, \quad \varpi'_1(x) = 0, \quad \varpi_2(x) = 0,$$

et ainsi de suite. Ces cas particuliers ne pourront donc jamais se présenter que si l'équation finale a des racines égales.

Extension au cas de plusieurs équations.

La même méthode, où l'on peut éviter les considérations géométriques que j'ai cru devoir employer pour plus de clarté, s'applique au cas d'un nombre quelconque d'équations entre un pareil nombre d'inconnues.

Soient, par exemple, trois équations à trois inconnues x, y, z, savoir :

$$(1) \quad f(x, y, z) = 0, \quad F(x, y, z) = 0, \quad \varphi(x, y, z) = 0;$$

on posera

$$(2) \quad t = x + \alpha y + 6z,$$

t étant une nouvelle variable, α et 6 deux indéterminées, et l'on portera dans les équations (1) la valeur de x, tirée de l'équation (2) : on aura ainsi trois équations,

$$(3) \begin{cases} f(t - \alpha y - 6z, y, z) = 0, \quad F(t - \alpha y - 6z, y, z) = 0, \\ \varphi(t - \alpha y - 6z, y, z) = 0, \end{cases}$$

entre lesquelles on éliminera y et z par un moyen quelconque (*). Soit

(4) $$\psi(t, \alpha, 6) = 0$$

l'équation finale en t ainsi obtenue; on aura d'abord l'équation finale résultant de l'élimination de y et z entre les proposées, en faisant $t = x$, $\alpha = 0$, $6 = 0$; ce sera donc

(5) $$\psi(x, 0, 0) = 0.$$

Maintenant, pour avoir les valeurs y et z qui correspondent à chaque racine x de cette équation finale, on différentiera l'équation (4) par rapport à α, puis par rapport à 6; on tirera ainsi

(6) $$\left\{\begin{array}{l} \dfrac{dt}{d\alpha} = -\dfrac{\dfrac{d\psi}{d\alpha}}{\dfrac{d\psi}{dt}} = \psi_1(t, \alpha, 6), \\[2ex] \dfrac{dt}{d6} = -\dfrac{\dfrac{d\psi}{d6}}{\dfrac{d\psi}{dt}} = \psi_2(t, \alpha, 6). \end{array}\right.$$

D'ailleurs, en différentiant l'équation (2), on a

$$\frac{dt}{d\alpha} = y, \quad \frac{dt}{d6} = z;$$

faisant donc dans les équations (6) $\alpha = 0$, $6 = 0$, $t = x$, on aura

$$y = \psi_1(x, 0, 0), \quad z = \psi_2(x, 0, 0).$$

Comme dans le cas de deux équations, il ne sera pas nécessaire de connaître les termes de $\psi(t, \alpha, 6)$ qui dé-

(*) La méthode d'élimination par les fonctions symétriques sera étendue, dans une prochaine leçon, au cas d'un nombre quelconque d'équations.

passent le premier degré en α et 6; car, si l'on suppose

$$\psi(t, \alpha, 6) = \varpi(t) + \alpha\varpi_1(t) + 6\varpi_2(t) + \ldots,$$

on aura

$$\frac{d\psi}{d\alpha} = \varpi_1(t) + \ldots,$$

$$\frac{d\psi}{d6} = \varpi_2(t) + \ldots,$$

$$\frac{d\psi}{dt} = \varpi'(t) + \ldots;$$

par conséquent, l'équation finale en x sera

$$\varpi(x) = 0,$$

et les valeurs de y et z seront

$$y = -\frac{\varpi_1(x)}{\varpi'(x)}, \quad z = -\frac{\varpi_2(x)}{\varpi'(x)}.$$

Si à une même valeur x correspondaient deux valeurs de y et de z, les formules précédentes seraient en défaut; il faudrait alors opérer comme nous l'avons fait dans le cas de deux équations. Ces cas d'exception n'offrent aucune difficulté, et je ne crois pas nécessaire de nous y arrêter davantage.

Au lieu d'employer deux indéterminées α et 6, comme nous l'avons fait, on peut se borner à une seule, et poser

$$(7) \qquad t = x + \alpha y + \alpha^2 z;$$

on éliminera alors x, y et z entre cette équation et les proposées, et l'on aura une équation finale

$$(8) \qquad \psi(t, \alpha) = 0.$$

L'équation finale en x s'en déduira, comme précédemment, en faisant $\alpha = 0$, $t = x$; cette équation sera donc

$$\psi(x, 0) = 0.$$

Pour avoir y et z, on différentiera deux fois l'équation (7), par rapport à α; ce qui donnera

$$\frac{dt}{d\alpha} = y + 2\alpha z, \quad \frac{d^2t}{d\alpha^2} = 2z.$$

Cela posé, en différentiant l'équation (8), on trouve

$$(9)\qquad \frac{dt}{d\alpha} = -\frac{\dfrac{d\psi}{d\alpha}}{\dfrac{d\psi}{dt}} = \psi_1(t, \alpha),$$

d'où

$$(10)\qquad y + 2\alpha z = \psi_1(t, \alpha);$$

différentiant aussi cette équation (10) par rapport à α, on aura

$$2z = \frac{d\psi_1}{d\alpha} + \frac{d\psi_1}{dt}\frac{dt}{d\alpha},$$

ou, en remplaçant $\frac{dt}{d\alpha}$ par sa valeur tirée de l'équation (9),

$$(11)\qquad 2z = \frac{d\psi_1}{d\alpha} + \psi_1\frac{d\psi_1}{dt} = \psi_2(t, \alpha).$$

Enfin, faisant $\alpha = 0$, $t = x$, dans les équations (10) et (11), on aura

$$y = \psi_1(x, 0), \quad 2z = \psi_2(x, 0).$$

Il est facile de voir qu'il ne sera pas nécessaire de calculer l'équation (8) entièrement, et qu'il suffira d'en connaître les trois premiers termes.

Le problème dont nous venons de donner la solution, d'après M. Liouville, est compris, du moins lorsqu'il ne s'agit que de deux équations, dans un autre plus général considéré par Abel. Supposons qu'on ait deux équations

$$f(x, y) = 0, \quad F(x, y) = 0,$$

et qu'ayant éliminé y par un moyen quelconque, on ait trouvé cette équation finale

$$\varpi(x) = 0;$$

cette dernière exprimant la condition pour que les deux proposées où y sera alors l'inconnue aient une racine commune, la recherche de la valeur de y, qui correspond à une racine de l'équation finale en x, est ramenée à trouver la racine commune y aux deux équations données. C'est précisément la question qu'Abel s'est proposée, et qu'il a résolue dans un Mémoire publié dans les *Annales de Mathématiques* de Gergonne, tome XVII, et qui ne fait pas partie du Recueil de ses œuvres complètes. Nous allons exposer sommairement l'analyse de ce grand géomètre.

Méthode d'Abel pour déterminer la racine commune à deux équations.

Quand deux équations ont une racine commune, on peut déterminer cette racine par la méthode du plus grand commun diviseur; mais on peut aussi, comme Abel l'a fait voir, former immédiatement l'expression de cette racine commune par la méthode des fonctions symétriques : on peut encore, par le même procédé, déterminer une fonction rationnelle quelconque de cette racine commune.

Soient les deux équations

$$(1)\ f(y) = y^m + p_1 y^{m-1} + p_2 y^{m-2} + \ldots + p_{m-1} y + p_m = 0,$$
$$(2)\ F(y) = y^n + q_1 y^{n-1} + q_2 y^{n-2} + \ldots + q_{n-1} y + q_n = 0,$$

qui ont une racine commune y_1, mais qui n'ont que cette seule racine commune, et proposons-nous de calculer une fonction rationnelle et entière $\varphi(y_1)$ de cette racine.

Désignons par $y_1, y_2, \ldots, y_n$ les n racines de l'équation (2), et portons-les dans le premier membre de l'équation (1) $f(y)$; on aura ces n résultats

$$f(y_1),\quad f(y_2),\quad f(y_3),\ldots,\quad f(y_n),$$

dont le premier est nul. Faisons ensuite les produits $n-1$ à $n-1$ de ces n quantités, et désignons généralement par R_μ celui de ces produits qui ne contient pas le facteur $f(y_\mu)$; les quantités

$$R_1,\quad R_2,\quad R_3,\ldots, R_n,$$

seront toutes nulles, à l'exception de la première. Cela posé, on aura identiquement

$$R_1\varphi(y_1) = R_1\varphi(y_1) + R_2\varphi(y_2) + R_3\varphi(y_3) + \ldots + R_n\varphi(y_n)$$
$$= \sum R\varphi(y),$$

$$R_1 = R_1 + R_2 + R_3 + \ldots + R_n = \sum R,$$

d'où, par la division,

$$\varphi(y_1) = \frac{\Sigma R\varphi(y)}{\Sigma R},$$

le signe $\sum$ s'étendant à toutes les racines de l'équation (2). On voit que cette expression de $\varphi(y_1)$ est une fonction symétrique et rationnelle de toutes les racines de l'équation (2), et, par conséquent, on pourra la calculer par l'une des méthodes que nous avons exposées.

Tel est le principe de la méthode d'Abel; mais on peut, par un artifice ingénieux qu'il a indiqué, simplifier notablement le calcul de la fonction $\varphi(y_1)$. Soit $\theta(y)$ une fonction rationnelle quelconque dont nous nous réservons de déterminer ultérieurement la forme; on aura, de

même que précédemment,

$$R_1\theta(y_1)\varphi(y_1) = R_1\theta(y_1)\varphi(y_1) + R_2\theta(y_2)\varphi(y_2) + \ldots$$
$$+ R_n\theta(y_n)\varphi(y_n) = \sum R\theta(y)\varphi(y),$$
$$R_1\theta(y_1) = R_1\theta(y_1) + R_2\theta(y_2) + \ldots + R_n\theta(y_n)$$
$$= \sum R\theta(y),$$

d'où, par la division,

$$\varphi(y_1) = \frac{\Sigma R\theta(y)\varphi(y)}{\Sigma R\theta(y)}.$$

Cette nouvelle expression de $\varphi(y_1)$ est, comme la précédente, une fonction symétrique des racines de l'équation (2) et pourra être calculée de la même manière; mais elle devient plus simple, comme on va le voir, en disposant convenablement de la fonction indéterminée $\theta(y)$. Nous désignerons par $F'(y)$ la dérivée de $F(y)$, et nous poserons avec Abel,

$$\theta(y) = \frac{1}{F'(y)};$$

la valeur de $\varphi(y_1)$ sera alors

$$\varphi(y_1) = \frac{\sum \frac{R\varphi(y)}{F'(y)}}{\sum \frac{R}{F'(y)}}.$$

Cela posé, les quantités $R_1, R_2, \ldots, R_n$ peuvent s'exprimer rationnellement, la première à l'aide de y_1, la seconde à l'aide de y_2, etc., la dernière à l'aide de y_n. En effet, R_μ est une fonction symétrique des quantités $y_1, y_2, \ldots, y_n$, excepté y_μ, c'est-à-dire une fonction symétrique des racines de l'équation

$$\frac{F(y)}{y - y_\mu} = 0,$$

ou

$$y^{n-1} + \left.\begin{matrix} q_1 \\ + y_\mu \end{matrix}\right| y^{n-2} + \left.\begin{matrix} q_2 \\ + q_1 y_\mu \\ + y_\mu^2 \end{matrix}\right| y^{n-3} + \ldots = 0.$$

R_μ pourra donc s'exprimer sous forme rationnelle et entière à l'aide de y_μ et des quantités toutes connues qui entrent dans les équations (1) et (2), de la manière suivante:

$$R_\mu = \rho_0 + \rho_1 y_\mu + \rho_2 y_\mu^2 + \ldots + \rho_p y_\mu^p.$$

En outre, par l'un des procédés indiqués dans la deuxième leçon, on pourra chasser de l'expression de R_μ toutes les puissances de y_μ supérieures à la $(n-1)^{ième}$, en sorte que la valeur de R_μ aura finalement cette forme :

$$(3) \qquad R_\mu = \rho_0 + \rho_1 y_\mu + \rho_2 y_\mu^2 + \ldots + \rho_{n-1} y_\mu^{n-1};$$

et l'on déduira de cette équation les valeurs de R_1, $R_2, \ldots, R_n$, en donnant successivement à l'indice μ les valeurs $1, 2, 3, \ldots, n$.

La quantité $R_\mu \varphi(y_\mu)$ pourra également s'exprimer par un polynôme entier et rationnel par rapport à y_μ de degré $n-1$, et qu'on calculera aisément quand R_μ sera trouvé : soit donc

$$R_\mu \varphi(y_\mu) = t_0 + t_1 y_\mu + t_2 y_\mu^2 + \ldots + t_{n-1} y_\mu^{n-1}.$$

Mais par un théorème connu (*), si $\psi(y)$ désigne un polynôme quelconque du degré $n-1$, la somme

$$\sum \frac{\psi(y)}{F'(y)},$$

étendue aux racines $y_1, y_2, \ldots, y_n$ de l'équation

$$F(y) = 0,$$

(*) Ce théorème, qui résulte de la théorie de la décomposition d'une fraction rationnelle en fractions simples, sera démontré dans la leçon suivante.

a pour valeur le coefficient de y^{n-1} dans $\psi(y)$; on aura, d'après cela,

$$\sum \frac{R\varphi(y)}{F'(y)} = t_{n-1},$$

$$\sum \frac{R}{F'(y)} = \rho_{n-1},$$

et, par suite,

$$\varphi(y_1) = \frac{t_{n-1}}{\rho_{n-1}}. \tag{4}$$

Il suffit donc, pour avoir la valeur de notre fonction entière $\varphi(y_1)$, de calculer les coefficients de y^{n-1} dans R_μ et $R_\mu\,\varphi(y_\mu)$. Pour une autre fonction entière $\Phi(y_1)$, on aurait pareillement

$$\Phi(y_1) = \frac{T_{n-1}}{\rho_{n-1}},$$

T_{n-1} désignant le coefficient de y_μ^{n-1} dans $R_\mu\,\Phi(y_\mu)$; et, par suite, pour une fonction rationnelle $\frac{\Phi(y_1)}{\varphi(y_1)}$, on aura

$$\frac{\Phi(y_1)}{\varphi(y_1)} = \frac{T_{n-1}}{t_{n-1}}.$$

Si l'on veut seulement calculer y_1, il faudra faire $\varphi(y_1) = y_1$ dans l'équation (4); t_{n-1} sera alors le coefficient de y_μ^{n-1} dans $R_\mu y_\mu$: or, en multipliant l'équation (3) par y_μ, on trouve

$$R_\mu y_\mu = \rho_0 y_\mu + \rho_1 y_\mu^2 + \ldots + \rho_{n-2} y_\mu^{n-1} + \rho_{n-1} y_\mu^n,$$

et, en chassant y_μ^n à l'aide de l'équation (2),

$$y_\mu^n + q_1 y_\mu^{n-1} + q_2 y_\mu^{n-2} + \ldots + q_{n-1} y + q_n = 0;$$

on aura

$$R_\mu y_\mu = \ldots + (\rho_{n-2} - q_1 \rho_{n-1})\, y_\mu^{n-1},$$

et, par suite,

$$t_{n-1} = \rho_{n-2} - q_1 \rho_{n-1};$$

la valeur de y_1 sera donc

$$y_1 = \frac{\rho_{n-2} - q_1 \rho_{n-1}}{\rho_{n-1}} = \frac{\rho_{n-2}}{\rho_{n-1}} - q_1.$$

Par où l'on voit qu'il suffit, pour avoir y_1, de calculer dans R_μ les coefficients de y_μ^{n-1} et de y_μ^{n-2}.

C'est ici l'occasion de mentionner un beau théorème que Lagrange a démontré dans son célèbre Mémoire inséré parmi ceux de l'Académie de Berlin pour 1770 et 1771, et qui est relatif aux conditions nécessaires pour que deux équations aient plusieurs racines communes.

Théorème de Lagrange sur les conditions nécessaires pour que deux équations aient plusieurs racines communes.

L'objet de ce théorème est de faire connaître les conditions pour que deux équations algébriques aient deux, trois, etc., racines communes, quand on connaît la condition pour qu'elles en aient une. Voici en quoi il consiste.

Si $V = 0$ *exprime la condition pour que deux équations algébriques*

$$f(x) = x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0,$$
$$F(x) = x^n + q_1 x^{n-1} + q_2 x^{n-2} + \ldots + q_{n-1} x + q_n = 0,$$

aient une racine commune, V *désignant une fonction entière des coefficients* $p_1, p_2, \ldots, q_1, q_2, \ldots$, *les conditions nécessaires pour deux racines communes seront*

$$V = 0 \quad \text{et} \quad \frac{dV}{dp_m} = 0,$$

ou bien

$$V = 0 \quad \text{et} \quad \frac{dV}{dq_n} = 0;$$

pareillement les conditions nécessaires pour trois racines communes seront

$$V = 0, \quad \frac{dV}{dp_m} = 0, \quad \frac{d^2V}{dp_m^2} = 0,$$

ou bien

$$V = 0, \quad \frac{dV}{dq_n} = 0, \quad \frac{d^2V}{dq_n^2} = 0,$$

et ainsi de suite; en sorte qu'on obtiendra les conditions nécessaires pour μ racines communes, en joignant à l'équation nécessaire pour une seule racine commune les $\mu - 1$ équations qu'on en déduit en la différentiant $\mu - 1$ fois par rapport au dernier terme de l'une des deux équations proposées.

Voici comment Lagrange a démontré ce théorème. Remarquons d'abord qu'on obtiendra la condition

$$V = 0,$$

nécessaire pour que les équations

$$(1) \qquad f(x) = 0, \quad F(x) = 0$$

aient une racine commune, en éliminant x entre ces deux équations. Cela posé, considérons les deux équations

$$(2) \qquad f(x) = y, \quad F(x) = 0,$$

qui ne diffèrent des équations (1) qu'en ce que le dernier terme p_m de la première est remplacé par $p_m - y$; on obtiendra l'équation finale résultant de l'élimination de x entre les équations (2) en faisant ce même changement de p_m en $p_m - y$ dans l'équation $V = 0$; cette équation finale sera donc, d'après le théorème de Taylor,

$$(3) \qquad V - \frac{dV}{dp_m} y + \frac{d^2V}{dp_m^2} \frac{y^2}{1.2} - \frac{d^3V}{dp_m^3} \frac{y^3}{1.2.3} + \ldots = 0.$$

Pour que les équations (1) aient une, deux, trois, etc.,

racines communes, il faut et il suffit que l'équation (3) en y ait une, deux, trois, etc., racines nulles, c'est-à-dire que l'on ait

$$V = 0, \quad \frac{dV}{dp_m} = 0$$

pour deux racines communes; que l'on ait, en outre,

$$\frac{d^2V}{dp_m^2} = 0$$

pour trois racines communes, et ainsi de suite.

Exemple. — La condition pour que les deux équations

$$(4) \quad \begin{cases} x^3 + px^2 + qx + r = 0, \\ 3x^2 + 2px + q = 0 \end{cases}$$

aient une racine commune, est

$$(5) \quad 4q^3 + 27r^2 - 18pqr - p^2q^2 + 4p^3r = 0;$$

on obtiendra donc les conditions nécessaires pour deux racines communes, en joignant à l'équation (5) celle qu'on en déduit par la différentiation relative à q ou à r. En différentiant par rapport à r, on trouve

$$(6) \quad 27r - 9pq + 2p^3 = 0.$$

Les équations (5) et (6) expriment ainsi les conditions pour que la première des équations (4) ait deux racines communes avec sa dérivée, c'est-à-dire pour qu'elle ait trois racines égales.

CINQUIÈME LEÇON.

Developpement en fractions simples, d'une fraction rationnelle dont le dénominateur n'a pas de facteurs multiples. — Démonstration d'une formule d'analyse. — Méthode de M. Liouville pour former le développement d'une fraction rationnelle. — Cas des fractions rationnelles dont le dénominateur a des facteurs multiples.

Nous nous sommes appuyé, dans la dernière leçon, sur une formule que l'on peut déduire de la théorie de la décomposition des fractions rationnelles en fractions simples, ou qui, inversement, peut être prise pour le point de départ de cette théorie. Nous allons étudier en détail ce double point de vue. Nous commencerons par établir le développement en fractions simples d'une fraction rationnelle dont le dénominateur n'a pas de facteurs multiples, et nous en déduirons la formule dont nous venons de parler. Nous donnerons ensuite, de cette même formule, une démonstration directe due à M. Liouville, et nous exposerons la méthode qu'il en a déduite pour former le développement d'une fraction rationnelle. Nous ferons voir, enfin, comment on peut passer du cas des fractions rationnelles dont le dénominateur n'a que des facteurs simples, au cas des fractions dont le dénominateur a des facteurs multiples.

Développement d'une fraction rationnelle en fractions simples.

Théorème. — *Soient*

$$f(x) = (x-a)(x-b)(x-c)\ldots(x-l)$$

un polynôme du degré m dont toutes les racines a, b,

$c, \ldots, l$ sont inégales, et $F(x)$ un polynôme du degré $m-1$ au plus; il y aura un système de valeurs des constantes $A, B, C, \ldots, L$, tel que l'on aura identiquement

$$(1) \qquad \frac{F(x)}{f(x)} = \frac{A}{x-a} + \frac{B}{x-b} + \frac{C}{x-c} + \ldots + \frac{L}{x-l},$$

et il n'y en aura qu'un seul.

L'équation (1) peut s'écrire ainsi :

$$(2) \qquad F(x) = \frac{Af(x)}{x-a} + \frac{Bf(x)}{x-b} + \ldots + \frac{Lf(x)}{x-l};$$

et si l'on admet qu'elle soit identique, elle sera satisfaite quand on donnera à x les valeurs $a, b, c, \ldots, l$; mais pour $x=a$, tous les termes du second membre sont nuls, à l'exception du premier $A\frac{f(x)}{x-a}$, qui se réduit à $Af'(a)$: on a donc

$$F(a) = Af'(a), \quad \text{d'où} \quad A = \frac{F(a)}{f'(a)}.$$

L'équation (2), ou, ce qui est la même chose, l'équation (1) ne peut donc avoir lieu identiquement que si l'on a

$$(3) \qquad A = \frac{F(a)}{f'(a)}, \quad B = \frac{F(b)}{f'(b)}, \ldots, \quad L = \frac{F(l)}{f'(l)};$$

ces valeurs de A, B, etc., sont les seules qui puissent remplir la condition demandée. Pour prouver qu'elles la remplissent en effet, remarquons qu'en les adoptant, l'équation (2) sera satisfaite pour les m valeurs $a, b, c, \ldots, l$ de x, et sera par conséquent identique, puisque son degré est $m-1$ au plus : d'ailleurs, les valeurs trouvées pour A, B, etc., sont finies, car les racines a, b, etc., sont inégales. On a donc le développement suivant pour

la fraction rationnelle $\frac{F(x)}{f(x)}$:

$$\frac{F(x)}{f(x)} = \frac{F(a)}{f'(a)}\frac{1}{x-a} + \frac{F(b)}{f'(b)}\frac{1}{x-b} + \ldots + \frac{F(l)}{f'(l)}\frac{1}{x-l}.$$

Supposons maintenant que le numérateur de la fraction rationnelle $\frac{F(x)}{f(x)}$ soit de degré supérieur à celui du dénominateur. Désignons par $\varpi(x)$ le quotient de la division de $F(x)$ par $f(x)$, et par $\varphi(x)$ le reste : on aura

$$\frac{F(x)}{f(x)} = \varpi(x) + \frac{\varphi(x)}{f(x)} = \varpi(x) + \frac{\varphi(a)}{f'(a)}\frac{1}{x-a} + \ldots + \frac{\varphi(l)}{f'(l)}\frac{1}{x-l};$$

mais, à cause de $F(x) = \varpi(x)\, f(x) + \varphi(x)$, on a

$$\varphi(a) = F(a), \quad \varphi(b) = F(b), \ldots,$$

donc

$$\frac{F(x)}{f(x)} = \varpi(x) + \frac{F(a)}{f'(a)}\frac{1}{x-a} + \frac{F(b)}{f'(b)}\frac{1}{x-b} + \ldots + \frac{F(l)}{f'(l)}\frac{1}{x-l}.$$

On voit que, dans ce cas, le développement conserve la même forme; il faut seulement ajouter le quotient entier de la division du numérateur par le dénominateur.

Démonstration d'une formule d'analyse.

L'équation

$$F(x) = \frac{F(a)}{f'(a)}\frac{f(x)}{x-a} + \frac{F(b)}{f'(b)}\frac{f(x)}{x-b} + \ldots + \frac{F(l)}{f'(l)}\frac{f(x)}{x-l},$$

ayant lieu identiquement si F est de degré inférieur à f, les coefficients de x^{m-1} sont égaux dans les deux membres ; si donc on désigne par P le coefficient de x^{m-1} dans $F(x)$, on aura

$$P = \frac{F(a)}{f'(a)} + \frac{F(b)}{f'(b)} + \ldots + \frac{F(l)}{f'(l)},$$

ou

$$\sum \frac{F(x)}{f'(x)} = P.$$

Dans cette formule, $f(x)$ désigne un polynôme quelconque de degré m, dont le premier terme a pour coefficient l'unité, $f'(x)$ sa dérivée, et $F(x)$ un polynôme quelconque de degré inférieur à m, dans lequel le coefficient de x^{m-1} est égal à P. Quant au signe $\sum$, il s'étend à toutes les racines de $f(x) = 0$. Cette formule est celle sur laquelle nous nous sommes appuyé dans la leçon précédente, et que nous avions admise sans la démontrer. Si le polynôme $F(x)$ est du degré $m - 2$ au plus, on aura $P = 0$, et, par suite,

$$\sum \frac{F(x)}{f'(x)} = 0.$$

Méthode de M. Liouville.

M. Liouville a déduit de l'équation précédente un moyen ingénieux de présenter la théorie de la décomposition des fractions rationnelles (*). Nous allons exposer ici cette méthode.

Soient $f(x)$ et $F(x)$ deux polynômes des degrés m et $m - 1$ respectivement, ayant pour valeurs

$$f(x) = x^m + px^{m-1} + \ldots,$$
$$F(x) = Px^{m-1} + \ldots,$$

et considérons l'équation

$$(1) \qquad f(x) + \alpha F(x) = 0,$$

où α désigne une indéterminée qui n'entre ni dans f, ni

(*) *Journal de Mathématiques pures et appliquées*, tome XI, page 462.

dans F; représentons par la notation $\sum x$ la somme des racines de l'équation (1), on aura

$$\sum x = -p - \mathrm{P}\alpha, \tag{2}$$

et ces racines étant des fonctions de α, on aura, en différentiant l'équation (2) par rapport à α,

$$\sum \frac{dx}{d\alpha} = -\mathrm{P}. \tag{3}$$

On a aussi, en différentiant l'équation (1) par rapport à α, et dénotant les dérivées à la manière ordinaire,

$$[f'(x) + \alpha \mathrm{F}'(x)]\frac{dx}{d\alpha} + \mathrm{F}(x) = 0;$$

d'où

$$\frac{dx}{d\alpha} = -\frac{\mathrm{F}(x)}{f'(x) + \alpha \mathrm{F}'(x)}.$$

On pourra donc écrire l'équation (3) de la manière suivante :

$$\sum \frac{\mathrm{F}(x)}{f'(x) + \alpha \mathrm{F}'(x)} = \mathrm{P}.$$

Dans cette équation, le signe $\sum$ s'étend à toutes les racines de l'équation (1), et l'on peut considérer α comme une quantité entièrement arbitraire; faisant donc $\alpha = 0$, on aura

$$\sum \frac{\mathrm{F}(x)}{f'(x)} = \mathrm{P},$$

le signe $\sum$ s'étendant alors aux racines de l'équation

$$f(x) = 0.$$

Si f étant toujours du degré m, F n'est que du degré $m-2$

au plus, P sera nul, et l'on aura

$$\sum \frac{F(x)}{f'(x)} = 0.$$

Voici, maintenant, comment M. Liouville déduit de cette dernière formule le théorème relatif au développement d'une fraction rationnelle.

Soient $F(x)$ un polynôme du degré $m-1$ au plus, $f(x)$ un polynôme du degré m, tel que

$$f(x) = (x-a)(x-b), \ldots, (x-l),$$

et posons

$$\varphi(x) = (x-t) f(x);$$

le degré du polynôme $\varphi(x)$ surpassant de deux unités au moins celui de $F(x)$, on aura, d'après le théorème qui vient d'être établi,

$$\sum \frac{F(x)}{\varphi'(x)} = 0,$$

ou, comme $a, b, c, \ldots, l$ et t sont les racines de $\varphi(x) = 0$,

$$(4) \qquad \frac{F(t)}{\varphi'(t)} + \frac{F(a)}{\varphi'(a)} + \frac{F(b)}{\varphi'(b)} + \ldots + \frac{F(l)}{\varphi'(l)} = 0.$$

Cela posé, en différentiant l'équation

$$\varphi(x) = (x-t) f(x),$$

on trouve

$$\varphi'(x) = (x-t) f'(x) + f(x);$$

on aura donc

$$\varphi'(t) = f(t)$$

et

$$\varphi'(a) = (a-t) f'(a), \quad \varphi'(b) = (b-t) f'(b), \ldots.$$

D'après cela, l'équation (4) donnera

$$\frac{F(t)}{f(t)} = \frac{F(a)}{f'(a)} \frac{1}{t-a} + \frac{F(b)}{f'(b)} \frac{1}{t-b} + \ldots + \frac{F(l)}{f'(l)} \frac{1}{t-l},$$

ce qui est précisément la formule à laquelle nous avons été conduit par la première méthode.

Cas des fractions rationnelles dont le dénominateur a des facteurs multiples.

Du développement que nous venons de trouver pour une fraction rationnelle dont le dénominateur n'a que des facteurs simples, on peut déduire celui d'une fraction dont le dénominateur a des facteurs multiples, en employant un artifice qui nous a déjà servi dans une précédente leçon.

Supposons, par exemple, que parmi les m racines $a, b, c, \ldots, k, l$ de l'équation $f(x)=0$, deux soient égales entre elles, que l'on ait $b=a$, mais que toutes les autres soient inégales et différentes de a, et soit toujours $F(x)$ un polynôme de degré inférieur à celui de $f(x)$; il s'agit de trouver le développement de la fraction $\frac{F(x)}{f(x)}$. Nous prendrons d'abord, au lieu de $f(x)$, un polynôme $\varphi(x)$, qu'on déduira de $f(x)$ en remplaçant l'une des deux racines a par une racine peu différente $a+h$; nous poserons, en un mot,

$$\varphi(x)=\frac{f(x)(x-a-h)}{x-a},$$

et alors nous aurons pour le développement de la fraction $\frac{F(x)}{\varphi(x)}$,

$$\frac{F(x)}{\varphi(x)}=\frac{F(a)}{\varphi'(a)}\frac{1}{x-a}+\frac{F(a+h)}{\varphi'(a+h)}\frac{1}{x-a-h}+\ldots+\frac{F(l)}{\varphi'(l)}\frac{1}{x-l}.$$

On a d'ailleurs

$$\frac{1}{x-a-h}=\frac{1}{x-a}+\frac{h}{(x-a)^2}+\frac{h^2}{(x-a)^3}+\ldots;$$

donc

$$\frac{F(x)}{\varphi(x)} = \left[\frac{F(a)}{\varphi'(a)} + \frac{F(a+h)}{\varphi'(a+h)}\right]\frac{1}{x-a}$$
$$+ \frac{hF(a+h)}{\varphi'(a+h)}\left[\frac{1}{(x-a)^2} + \frac{h}{(x-a)^3} + \ldots\right]$$
$$+ \frac{F(c)}{\varphi'(c)}\frac{1}{x-c} + \ldots + \frac{F(l)}{\varphi'(l)}\frac{1}{x-l}.$$

Mais la dérivée $\varphi'(x)$ de $\varphi(x)$ a pour valeur

$$\varphi'(x) = \frac{f'(x)(x-a-h)}{x-a} + \frac{f(x)}{x-a} - \frac{f(x)(x-a-h)}{(x-a)^2};$$

d'où, en faisant successivement $x = a$ et $x = a + h$, et se rappelant que $f(x)$ a deux racines égales à a,

$$\varphi'(a) = -\frac{hf''(a)}{2}, \quad \varphi'(a+h) = \frac{f(a+h)}{h} = \frac{hf''(a)}{2},$$

en négligeant dans $\varphi'(a+h)$ les puissances de h supérieures à la première. On aura, d'après cela, en négligeant partout les puissances de h supérieures à la première,

$$\frac{F(x)}{\varphi'(x)} = \frac{2}{f''(a)}\left[\frac{F(a+h)-F(a)}{h}\right]\frac{1}{x-a} + \frac{2F(a)}{f''(a)}\frac{1}{(x-a)^2}$$
$$+ \frac{F(c)}{\varphi'(c)}\frac{1}{x-c} + \ldots + \frac{F(l)}{\varphi'(l)}\frac{1}{x-l}\cdots$$

Cette égalité n'est pas exacte, mais elle le sera à la limite pour $h = 0$, auquel cas $\varphi(x) = f(x)$; on aura donc

$$\frac{F(x)}{f(x)} = \frac{2F'(a)}{f''(a)}\frac{1}{x-a} + \frac{2F(a)}{f''(a)}\frac{1}{(x-a)^2} + \frac{F(c)}{f'(c)}\frac{1}{x-c} + \ldots$$
$$+ \frac{F(l)}{f'(l)}\frac{1}{x-l}.$$

On voit aisément comment il faudrait opérer dans le cas où $f(x)$ aurait trois ou un plus grand nombre de

racines égales à a. Mais nous n'insisterons pas davantage sur cette méthode, de laquelle il ne semble pas qu'on puisse déduire un procédé commode pour déterminer généralement l'expression algébrique des différents termes du développement; il nous suffit d'avoir montré, par ce qui précède, que le développement de $\frac{F(x)}{f(x)}$, dans le cas où les racines de $f(x)$ sont inégales, n'est pas aussi particulier qu'on aurait pu le croire, et qu'il renferme implicitement tous les cas.

SIXIÈME LEÇON.

Théorie générale de la décomposition des fractions rationnelles en fractions simples. — Théorèmes sur la possibilité du développement. — Méthodes pour former le développement.

Théorie générale de la décomposition des fractions rationnelles en fractions simples.

Nous avons été conduit naturellement, par une question incidente, à nous occuper de la décomposition des fractions rationnelles en fractions simples. Les détails dans lesquels nous sommes entré à ce sujet, suffisent pour l'objet que nous avions en vue; mais la théorie des fractions rationnelles est si importante, et ses applications dans l'analyse mathématique si variées, que je crois utile de la reprendre ici, en lui donnant tous les développements qu'elle comporte.

Nous commencerons par établir qu'une fraction rationnelle $\frac{F(x)}{f(x)}$, dont les deux termes sont des polynômes quelconques premiers entre eux, est décomposable en une partie entière (qui peut être nulle), et en plusieurs *fractions simples* à numérateurs constants, ayant pour dénominateurs les diverses puissances des facteurs linéaires qui peuvent diviser le polynôme $f(x)$. Nous démontrerons ensuite qu'une fraction rationnelle n'est décomposable ainsi que d'une seule manière, et nous indiquerons enfin le moyen de former son développement.

Théorèmes sur la possibilité du développement d'une fraction rationnelle.

THÉORÈME I. — *Si a désigne une racine de l'équation $f(x)=0$, α son degré de multiplicité, en sorte que l'on ait*

$$f(x)=(x-a)^\alpha f_1(x),$$

$f_1(x)$ étant un polynôme non divisible par $x-a$, la fraction rationnelle $\frac{F(x)}{f(x)}$ pourra toujours être décomposée en deux parties de la manière suivante:

$$\frac{F(x)}{f(x)}=\frac{A}{(x-a)^\alpha}+\frac{F_1(x)}{(x-a)^{\alpha-1}f_1(x)},$$

A étant une constante, et $F_1(x)$ un polynôme entier et rationnel.

En effet, on a identiquement, et quel que soit A,

$$\frac{F(x)}{f(x)}=\frac{F(x)}{(x-a)^\alpha f_1(x)}=\frac{A}{(x-a)^\alpha}+\frac{F(x)-Af_1(x)}{(x-a)^\alpha f_1(x)},$$

et pour que le deuxième terme du second membre ne contienne à son dénominateur que la puissance $\alpha-1$ du facteur $x-a$, il faut et il suffit que le numérateur $F(x)-Af_1(x)$ s'annule pour $x=a$. Posons donc

$$F(a)-Af_1(a)=0,\quad \text{d'où}\quad A=\frac{F(a)}{f_1(a)};$$

cette valeur de A sera finie, puisque $f_1(a)$ n'est pas nul, et si l'on fait

$$F(x)-Af_1(x)=(x-a)F_1(x),$$

on aura

$$\frac{F(x)}{f(x)}=\frac{A}{(x-a)^\alpha}+\frac{F_1(x)}{(x-a)^{\alpha-1}f_1(x)},$$

ce qu'il fallait démontrer

Corollaire. — En appliquant le même théorème à la fraction $\frac{F_1(x)}{(x-a)^{\alpha-1} f_1(x)}$, on pourra la mettre sous la forme

$$\frac{A_1}{(x-a)^{\alpha-1}} + \frac{F_2(x)}{(x-a)^{\alpha-2} f_1(x)},$$

A_1 étant une constante et $F_2(x)$ une fonction entière; seulement ici A_1 peut être nulle, car $F_1(x)$ peut admettre le facteur $x-a$. En continuant ainsi, on voit que la fraction rationnelle $\frac{F(x)}{f(x)}$ peut être décomposée de la manière suivante :

$$\frac{F(x)}{f(x)} = \frac{F(x)}{(x-a)^{\alpha} f_1(x)} = \frac{A}{(x-a)^{\alpha}} + \frac{A_1}{(x-a)^{\alpha-1}} + \ldots + \frac{A_{\alpha-1}}{x-a} + \frac{F_{\alpha}(x)}{f_1(x)},$$

A, A_1, A_2, etc., étant des constantes finies et déterminées dont la première n'est pas nulle, et $F_{\alpha}(x)$ une fonction entière.

Soient maintenant b une seconde racine de $f(x) = 0$ et 6 son degré de multiplicité, en sorte que l'on ait

$$f_1(x) = (x-b)^{6} f_2(x);$$

en appliquant la formule précédente à la fraction $\frac{F_{\alpha}(x)}{f_1(x)}$, on aura une valeur de la forme

$$\frac{F_{\alpha}(x)}{f_1(x)} = \frac{F_{\alpha}(x)}{(x-b)^{6} f_2(x)} = \frac{B}{(x-b)^{6}} + \frac{B_1}{(x-b)^{6-1}} + \ldots + \frac{B_{6-1}}{x-b} + \frac{F_{6}(x)}{f_2(x)},$$

et, par suite,

$$\frac{F(x)}{f(x)} = \frac{A}{(x-a)^\alpha} + \frac{A_1}{(x-a)^{\alpha-1}} + \ldots + \frac{A_{\alpha-1}}{x-a}$$
$$+ \frac{B}{(x-b)^6} + \frac{B_1}{(x-b)^{6-1}} + \ldots + \frac{B_{6-1}}{x-b} + \frac{F_6(x)}{f_2(x)},$$

B, B_1, etc., étant des constantes déterminées dont la première n'est pas nulle, et $F_6(x)$ une fonction entière.

Il résulte de là, qu'en général, si l'on suppose

$$f(x) = (x-a)^\alpha (x-b)^6 \ldots (x-c)^\gamma,$$

la fraction rationnelle $\frac{F(x)}{f(x)}$ pourra être développée de la manière suivante:

$$\frac{F(x)}{f(x)} = \frac{A}{(x-a)^\alpha} + \frac{A_1}{(x-a)^{\alpha-1}} + \ldots + \frac{A_{\alpha-1}}{x-a},$$
$$+ \frac{B}{(x-b)^6} + \frac{B_1}{(x-b)^{6-1}} + \ldots + \frac{B_{6-1}}{x-b},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$+ \frac{C}{(x-c)^\gamma} + \frac{C_1}{(x-c)^{\gamma-1}} + \ldots + \frac{C_{\gamma-1}}{x-c} + E(x),$$

A, A_1, ..., B, B_1, ..., C, C_1, ..., étant des constantes finies, et $E(x)$ une fonction entière. C'est précisément la proposition qu'il s'agissait d'établir.

Au lieu de s'occuper d'abord des fractions simples relatives à la racine a, on aurait pu commencer par celles qui se rapportent à une autre racine, b par exemple; mais, comme nous allons le faire voir, on aurait toujours trouvé le même développement.

THÉORÈME II. — *Une fraction rationnelle n'est dé-*

composable que d'une seule manière en une partie entière et en fractions simples.

Supposons qu'on ait trouvé deux développements d'une même fraction rationnelle,

$$\frac{A}{(x-a)^{\alpha}} + \ldots + \frac{B}{(x-b)^{6}} + \ldots + E(x)$$

et

$$\frac{A'}{(x-a)^{\alpha'}} + \ldots + \frac{B'}{(x-b)^{6'}} + \ldots + E'(x);$$

on aura

$$\frac{A}{(x-a)^{\alpha}} + \ldots + E(x) = \frac{A'}{(x-a)^{\alpha'}} + \ldots + E'(x).$$

Cela posé, α et α' étant respectivement les exposants des plus hautes puissances de $x-a$, dans les deux membres, je dis que $\alpha=\alpha'$ et $A=A'$. Supposons, en effet, que α et α' soient inégaux et que α soit le plus grand; tirons de l'équation précédente la valeur de $\frac{A}{(x-a)^{\alpha}}$, et réduisons tous les autres termes au même dénominateur; on aura

$$\frac{A}{(x-a)^{\alpha}} = \frac{\varphi(x)}{(x-a)^{\alpha-1}\psi(x)},$$

ou

$$A = (x-a)\frac{\varphi(x)}{\psi(x)},$$

φ et ψ désignant des polynômes dont le second n'est pas divisible par $x-a$. D'ailleurs A est une constante; il faut donc qu'elle soit nulle, car l'équation précédente donne $A=0$ pour $x=a$. Si donc A n'est pas nul, on ne peut supposer $\alpha>\alpha'$, et l'on ferait voir de même que, si A' n'est pas nul, on ne peut supposer non plus $\alpha<\alpha'$; on a donc $\alpha=\alpha'$. Je dis maintenant que $A=A'$. En effet, de

l'équation entre les deux développements on tirera, α' étant égal à α,

$$\frac{A - A'}{(x-a)^{\alpha}} = \frac{\varphi(x)}{(x-a)^{\alpha-1}\psi(x)},$$

ou

$$A - A' = (x-a)\frac{\varphi(x)}{\psi(x)},$$

φ et ψ étant, comme précédemment, des polynômes don le second n'est pas divisible par $x-a$; comme $A - A'$ est constant, et que sa valeur est nulle pour $x = a$, d'après l'équation précédente, on aura $A = A'$.

Les termes qui renferment la plus haute puissance de $x - a$ en dénominateur, dans les deux développements, étant égaux entre eux, on pourra les ôter de part et d'autre, et les deux restés seront égaux. En raisonnant sur eux comme sur les proposés, on fera voir que les termes qui contiennent en dénominateur la plus haute puissance du même binôme $x - a$, ou d'un autre binôme, sont aussi égaux entre eux; et en continuant ainsi, on prouvera que les fractions simples des deux développements sont égales chacune à chacune : il en résultera par conséquent l'égalité des parties entières $E(x)$ et $E'(x)$.

Corollaire. — La partie entière du développement d'une fraction rationnelle $\frac{F(x)}{f(x)}$ en fractions simples étant indépendante du moyen qu'on emploie pour faire ce développement, on l'obtiendra en faisant la division de $F(x)$ par $f(x)$; car si $\varphi(x)$ désigne le reste de cette division, $E(x)$ le quotient, on aura

$$\frac{F(x)}{f(x)} = E(x) + \frac{\varphi(x)}{f(x)}.$$

Or, le degré de $\varphi(x)$ étant moindre que celui de $f(x)$, le

développement de $\frac{\varphi(x)}{f(x)}$ ne contiendra évidemment pas de partie entière; donc, etc.

Méthodes pour former le développement d'une fraction rationnelle en fractions simples.

Le corollaire du théorème I, par lequel on démontre la possibilité du développement, donne aussi le moyen de former ce développement. Ainsi, dans le cas où les exposants $\alpha, \beta, \ldots, \gamma$ se réduisent tous à l'unité, on en déduit aisément la formule que nous avons obtenue dans la leçon précédente; mais, ce cas simple excepté, l'emploi de ce procédé exigerait des calculs fort pénibles.

On peut aussi employer la méthode des coefficients indéterminés; il faut alors calculer la partie entière du développement au moyen de la division du numérateur par le dénominateur, et l'on n'aura plus qu'à développer une fraction, dont le numérateur est de degré inférieur à celui du dénominateur; on égalera cette fraction au développement dont les coefficients seuls sont inconnus; on chassera les dénominateurs, et en égalant les coefficients des mêmes puissances de x dans les deux membres, on obtiendra une série d'équations qui serviront à déterminer les coefficients du développement.

EXEMPLE. — Soit à développer la fraction rationnelle $\frac{1}{x^3(x-1)}$ en fractions simples.

On posera

$$\frac{1}{x^3(x-1)} = \frac{A}{x^3} + \frac{B}{x^2} + \frac{C}{x} + \frac{D}{x-1},$$

d'où, en chassant les dénominateurs,

$$\begin{aligned} 1 &= A(x-1) + B(x^2-x) + C(x^3-x^2) + Dx^3 \\ &= -A + (A-B)x + (B-C)x^2 + (C+D)x^3, \end{aligned}$$

et, par conséquent,

$$-A=1,\quad A-B=0,\quad B-C=0,\quad C+D=0,$$

d'où

$$A=-1,\quad B=-1,\quad C=-1;\quad D=1,$$

et, par suite,

$$\frac{1}{x^3(x-1)}=-\frac{1}{x^3}-\frac{1}{x^2}-\frac{1}{x}+\frac{1}{x-1}.$$

Nous allons indiquer une autre méthode qui n'exige que l'emploi de la division algébrique.

Soit la fraction rationnelle $\frac{F(x)}{f(x)}$, dont le dénominateur $f(x)$ a pour valeur

$$f(x)=(x-a)^\alpha(x-b)^\beta\ldots(x-c)^\gamma;$$

cette fraction n'étant susceptible que d'un seul développement, on peut chercher, à part la partie entière, les fractions simples qui répondent à la racine a, puis celles qui répondent à la racine b, etc., et faire ensuite la somme de tous les résultats partiels ainsi obtenus.

La partie entière $E(x)$ s'obtiendra par la division de $F(x)$ par $f(x)$; voyons comment on peut obtenir les fractions simples qui répondent à chaque racine, à a par exemple. Soit

$$f(x)=(x-a)^\alpha f_1(x).$$

Posons $x=a+h$, ordonnons les polynômes $F(a+h)$ et $f_1(a+h)$ par rapport aux puissances croissantes de h, et faisons la division du premier par le second, en arrêtant le quotient au terme du degré $\alpha-1$ en h; soient

$$A+A_1h+A_2h^2+\ldots+A_{\alpha-1}h^{\alpha-1}$$

ce quotient, et $h^\alpha R$ le reste qui contient h^α à tous ses

termes, en sorte que R désigne ici une fonction entière de h; on aura

$$\frac{F(a+h)}{f_1(a+h)} = A + A_1 h + A_2 h^2 + \ldots + A_{\alpha-1} h^{\alpha-1} + \frac{h^\alpha R}{f_1(a+h)}.$$

Remplaçons dans cette égalité h par sa valeur $x-a$, puis divisons les deux membres par $(x-a)^\alpha$, et remarquons enfin que R se réduira à une fonction entière de x, $F_\alpha(x)$; on aura

$$\frac{F(x)}{f(x)} = \frac{F(x)}{(x-a)^\alpha f_1(x)}$$

$$= \frac{A}{(x-a)^\alpha} + \frac{A_1}{(x-a)^{\alpha-1}} + \frac{A_2}{(x-a)^{\alpha-2}} + \ldots + \frac{A_{\alpha-1}}{x-a} + \frac{F_\alpha(x)}{f_1(x)};$$

d'où il suit que la partie du développement de $\frac{F(x)}{f(x)}$, qui est relative à la racine a, sera

$$\frac{A}{(x-a)^\alpha} + \frac{A_1}{(x-a)^{\alpha-1}} + \ldots + \frac{A_{\alpha-1}}{x-a}.$$

On pourrait déterminer ainsi, indépendamment les unes des autres, les parties du développement qui se rapportent aux diverses racines, mais il sera plus simple d'appliquer la même méthode à la fraction $\frac{F_\alpha(x)}{f_1(x)}$ qui complète les termes déjà trouvés; on obtiendra ainsi les termes qui se rapportent à une seconde racine, et une troisième fraction sur laquelle on continuera l'opération.

La méthode précédente a surtout l'avantage de faire connaître l'expression algébrique des coefficients du développement. En effet, la division des polynômes $F(a+h)$ et $f_1(a+h)$, que nous avons effectuée, dans le but d'obtenir les coefficients $A_1, A_2, \ldots, A_\alpha$, revient évidemment

à développer la fonction $\frac{F(a+h)}{f_1(a+h)}$ en série ordonnée suivant les puissances croissantes de h, et comme une fonction n'est développable que d'une seule manière en une série de cette espèce, on obtiendra le même résultat en faisant usage de la formule de Maclaurin. Si donc on pose

$$\frac{F(x)}{f_1(x)} = \varphi(x),$$

on aura

$$\frac{F(a+h)}{f_1(a+h)} = \varphi(a+h) = \varphi(a) + h\varphi'(a) + h^2\frac{\varphi''(a)}{1.2} + \ldots$$
$$+ h^{\alpha-1}\frac{\varphi^{\alpha-1}(a)}{1.2\ldots(\alpha-1)} + h^\alpha R_1,$$

en désignant par $h^\alpha R_1$ le reste de la série; ici R_1 est une fonction rationnelle de h qui n'est point infinie pour $h=0$, et, par conséquent, cette valeur de $\frac{F(a+h)}{f_1(a+h)}$ est identique à celle trouvée précédemment. On aura donc

$$A = \varphi(a), \quad A_1 = \varphi'(a), \quad A_2 = \frac{\varphi''(a)}{1.2}, \ldots,$$
$$A_{\alpha-1} = \frac{\varphi^{\alpha-1}(a)}{1.2\ldots(\alpha-1)},$$

d'où résulte ce théorème général.

THÉORÈME. — *Si l'on a*

$$f(x) = (x-a)^\alpha (x-b)^6, \ldots, (x-c)^\gamma,$$

que $F(x)$ *désigne une fonction entière de* x, *dont le quotient par* $f(x)$ *soit* $E(x)$, *et que l'on fasse, pour abréger,*

$$\varphi(x) = (x-a)^\alpha \frac{F(x)}{f(x)}, \quad \psi(x) = (x-b)^6 \frac{F(x)}{f(x)}, \ldots,$$
$$\varpi(x) = (x-c)^\gamma \frac{F(x)}{f(x)},$$

on aura le développement suivant pour la fraction rationnelle $\frac{F(x)}{f(x)}$:

$$\frac{F(x)}{f(x)} = E(x)$$

$$+ \frac{\varphi(a)}{(x-a)^{\alpha}} + \frac{\varphi'(a)}{(x-a)^{\alpha-1}} + \frac{\varphi''(a)}{1.2(x-a)^{\alpha-2}} + \ldots + \frac{\varphi^{\alpha-1}(a)}{1.2\ldots(\alpha-1)(x-a)}$$

$$+ \frac{\psi(b)}{(x-b)^{6}} + \frac{\psi'(b)}{(x-b)^{6-1}} + \frac{\psi''(b)}{1.2.(x-b)^{6-2}} + \ldots + \frac{\psi^{6-1}(b)}{1.2\ldots(6-1)(x-b)}$$

. . . .

. . . .

$$+ \frac{\varpi(c)}{(x-c)^{\gamma}} + \frac{\varpi'(c)}{(x-c)^{\gamma-1}} + \frac{\varpi''(c)}{1.2(x-c)^{\gamma-2}} + \ldots + \frac{\varpi^{\gamma-1}(c)}{1.2\ldots(\gamma-1)(x-c)}.$$

La théorie qui vient d'être exposée subsiste entièrement si quelques-unes des racines de $f(x) = 0$ sont imaginaires, mais le développement de $\frac{F(x)}{f(x)}$ est alors compliqué d'imaginaires. On a cherché à modifier, dans ce cas, la forme de ce développement, de manière à n'y introduire que des quantités réelles, et on y est parvenu par une méthode que nous exposerons dans la leçon suivante.

SEPTIÈME LEÇON.

Developpement particulier pour les fractions rationnelles dont le dénominateur a des facteurs linéaires imaginaires. — Conditions pour qu'une différentielle rationnelle ait une intégrale algébrique. — Détermination du terme général d'une série récurrente.

Développement particulier pour les fractions rationnelles dont le dénominateur a des facteurs linéaires imaginaires.

La possibilité de ce nouveau développement résulte du théorème suivant :

THÉORÈME I. — *Si x^2+px+q est le produit de deux facteurs imaginaires conjugués du polynôme réel $f(x)$, n la plus haute puissance de ce trinôme qui divise $f(x)$, en sorte qu'on ait*

$$f(x) = (x^2+px+q)^n f_1(x),$$

la fraction réelle et rationnelle $\frac{F(x)}{f(x)}$ pourra se décomposer en deux parties, de la manière suivante :

$$\frac{F(x)}{f(x)} = \frac{Px+Q}{(x^2+px+q)^n} + \frac{F_1(x)}{(x^2+px+q)^{n-1}f_1(x)},$$

P et Q étant des constantes réelles, et $F_1(x)$ un polynôme réel.

On a identiquement

$$\frac{F(x)}{f(x)} = \frac{F(x)}{(x^2+px+q)^n f_1(x)}$$

$$= \frac{Px+Q}{(x^2+px+q)^n} + \frac{F(x)-(Px+Q)f_1(x)}{(x^2+px+q)^n f_1(x)},$$

et l'on peut déterminer P et Q de manière que le numérateur de la deuxième partie du second membre soit divisible par $x^2 + px + q$, c'est-à-dire de manière que ce numérateur s'annule en remplaçant x par chacune des racines de l'équation

$$x^2 + px + q = 0.$$

Soient $h + k\sqrt{-1}$ et $h - k\sqrt{-1}$ ces deux racines, et posons

$$F(h \pm k\sqrt{-1}) - [P(h \pm k\sqrt{-1}) + Q] f_1(h \pm k\sqrt{-1}) = 0;$$

on tirera de là

$$P(h \pm k\sqrt{-1}) + Q = \frac{F(h \pm k\sqrt{-1})}{f_1(h \pm k\sqrt{-1})} = M \pm N\sqrt{-1},$$

M et N étant des quantités réelles dont les valeurs sont finies et déterminées, puisque, par hypothèse, $f_1(x)$ n'est pas divisible par $x^2 + px + q$. L'équation précédente se décompose dans les deux suivantes,

$$Ph + Q = M, \quad Pk = N,$$

qui donnent pour P et Q, ces deux valeurs réelles et finies,

$$P = \frac{N}{k}, \quad Q = \frac{Mk - Nh}{k}.$$

Les valeurs de P et Q étant ainsi déterminées, nous poserons

$$\frac{F(x) - (Px + Q) f_1(x)}{x^2 + px + q} = F_1(x),$$

$F_1(x)$ désignant un polynôme réel, et, par suite, on aura

$$\frac{F(x)}{(x^2 + px + q)^n f_1(x)} = \frac{Px + Q}{(x^2 + px + q)^n} + \frac{F_1(x)}{(x^2 + px + q)^{n-1} f_1(x)},$$

ce qu'il fallait démontrer.

Corollaire. — On voit, par là, que la fraction rationnelle $\frac{F(x)}{f(x)}$ pourra se décomposer de la manière suivante :

$$\frac{F(x)}{f(x)} = \frac{Px+Q}{(x^2+px+q)^n} + \frac{P_1x+Q_1}{(x^2+px+q)^{n-1}} + \ldots$$
$$\ldots + \frac{P_{n-1}x+Q_{n-1}}{x^2+px+q} + \frac{F_n(x)}{f_1(x)},$$

P, Q, P_1, Q_1, etc., désignant des constantes réelles, et $F_n(x)$ un polynôme réel aussi. Et en combinant le théorème précédent avec le théorème analogue démontré dans la dernière leçon, on obtient celui-ci :

Théorème II. — *Si l'on décompose le polynôme $f(x)$ en facteurs réels du premier et du second degré, en sorte qu'on ait*

$$f(x) = (x-a)^{\alpha}(x-b)^{6}\ldots(x-c)^{\gamma}(x^2+px+q)^{n}\ldots(x^2+rx+s)^{m},$$

on pourra développer la fraction rationnelle $\frac{F(x)}{f(x)}$ de la manière suivante :

$$\frac{F(x)}{f(x)} = E(x) + \frac{A}{(x-a)^{\alpha}} + \frac{A_1}{(x-a)^{\alpha-1}} + \ldots + \frac{A_{\alpha-1}}{x-a},$$
$$+ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$+ \frac{C}{(x-c)^{\gamma}} + \frac{C_1}{(x-c)^{\gamma-1}} + \ldots + \frac{C_{\gamma-1}}{x-c}$$
$$+ \frac{Px+Q}{(x^2+px+q)^{n}} + \frac{P_1x+Q_1}{(x^2+px+q)^{n-1}} + \ldots + \frac{P_{n-1}x+Q_{n-1}}{x^2+px+q}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$+ \frac{Rx+S}{(x^2+rx+s)^{m}} + \frac{R_1x+S_1}{(x^2+rx+s)^{m-1}} + \ldots + \frac{R_{m-1}x+S_{m-1}}{x^2+rx+s},$$

$E(x)$ désignant une partie entière qui peut être nulle, et $A, A_1, \ldots, C, C_1, \ldots, P, Q, P_1, Q_1, \ldots, R, S, R_1, S_1, \ldots,$ des constantes réelles.

Théorème III. — *Une fraction rationnelle n'est décomposable que d'une seule manière en fractions simples de la forme qu'on vient de considérer.*

Soient deux développements d'une même fraction rationnelle. On démontrera, comme nous l'avons fait dans la leçon précédente, l'égalité des fractions simples qui correspondent aux facteurs du premier degré du dénominateur, et quant à celle des fractions simples qui correspondent aux facteurs du second degré, elle se démontre d'une manière analogue, comme nous allons voir. Soient $\frac{Px+Q}{(x^2+px+q)^n}$ le terme dont le dénominateur contient la plus haute puissance de x^2+px+q dans le premier développement, et $\frac{P'x+Q'}{(x^2+px+q)^{n'}}$, le terme analogue dans le second. Je dis d'abord que $n'=n$. Supposons, en effet, que cela ne soit pas, et que $n>n'$: de l'égalité qui a lieu entre les deux développements, tirons la valeur de $\frac{Px+Q}{(x^2+px+q)^n}$; cette valeur sera exprimée par une somme de quantités dont aucune n'a en dénominateur une puissance de x^2+px+q supérieure à $n-1$. En réduisant donc toutes ces quantités au même dénominateur, on aura une égalité de la forme

$$\frac{Px+Q}{(x^2+px+q)^n}=\frac{\varphi(x)}{(x^2+px+q)^{n-1}\psi(x)},$$

ou

$$Px+Q=(x^2+px+q)\frac{\varphi(x)}{\psi(x)},$$

$\varphi(x)$ et $\psi(x)$ désignant des polynômes, dont le second $\psi(x)$ n'est pas divisible par x^2+px+q. Or l'égalité précédente est impossible; car, autrement, l'équation $Px+Q=0$ devrait admettre les deux racines de l'équation $x^2+px+q=0$, ce qui ne peut arriver, à moins que P

et Q ne soient nuls en même temps, contrairement à l'hypothèse. On ne peut donc supposer $n > n'$ ni $n' > n$, pour une raison semblable; par conséquent, on a $n' = n$.

Je dis maintenant que l'on a aussi $P' = P$, $Q' = Q$. Reprenons, en effet, l'égalité qui a lieu par hypothèse entre les deux développements, mettons dans un même membre les deux termes $\frac{Px + Q}{(x^2 + px + q)^n}$ et $\frac{P'x + Q'}{(x^2 + px + q)^n}$, et dans le second membre tous les autres termes dont les dénominateurs ne contiendront aucune puissance de $x^2 + px + q$ supérieure à la $(n-1)^{ième}$; réduisant donc tous ces derniers termes au même dénominateur, on aura une égalité de cette forme

$$\frac{(P - P')x + (Q - Q')}{(x^2 + px + q)^n} = \frac{\varphi(x)}{(x^2 + px + q)^{n-1}\psi(x)},$$

ou

$$(P - P')x + (Q - Q') = (x^2 + px + q)\frac{\varphi(x)}{\psi(x)},$$

$\varphi(x)$ et $\psi(x)$ désignant, comme précédemment, des polynômes dont le second n'est pas divisible par $x^2 + px + q$, et l'on fera voir aussi, comme plus haut, que cette égalité exige

$$P = P', \quad Q = Q'.$$

Il suit de là que dans nos deux développements, les termes qui contiennent en dénominateur la plus haute puissance d'un facteur du second degré sont égaux; en supprimant ces deux termes, les deux restes auront encore, pour la même raison, deux termes égaux, et, en continuant ainsi, on voit que les deux développements proposés ne sont formés que de fractions simples égales chacune à chacune : il en résulte en même temps l'égalité des parties entières, s'il y en a.

Méthode de décomposition. — Pour trouver le déve-

loppement d'une fraction rationnelle $\frac{F(x)}{f(x)}$, on déterminera la partie entière et les fractions qui correspondent aux facteurs réels du premier degré du dénominateur, comme on l'a vu dans la leçon précédente. Quant aux fractions qui correspondent aux facteurs réels du second degré, on pourra les déterminer successivement par le procédé même qui nous a servi à démontrer le théorème I. On pourra aussi faire usage de la méthode des coefficients indéterminés.

Dans le cas où les racines imaginaires de l'équation $f(x) = 0$ sont toutes inégales, on peut déduire le nouveau développement de la fraction rationnelle $\frac{F(x)}{f(x)}$, de celui qui a été établi dans la cinquième leçon. Soient, en effet, $h + k\sqrt{-1}$ et $h - k\sqrt{-1}$ deux racines simples imaginaires et conjuguées de l'équation $f(x) = 0$; le développement de la fraction $\frac{F(x)}{f(x)}$ contiendra, comme on l'a vu dans la cinquième leçon, les deux termes suivants :

$$\frac{F(h + k\sqrt{-1})}{f'(h + k\sqrt{-1})} \cdot \frac{1}{x - h - k\sqrt{-1}},$$
$$\frac{F(h - k\sqrt{-1})}{f'(h - k\sqrt{-1})} \cdot \frac{1}{x - h + k\sqrt{-1}}.$$

La somme de ces deux termes est de la forme

$$\frac{P + Q\sqrt{-1}}{x - h - k\sqrt{-1}} + \frac{P - Q\sqrt{-1}}{x - h + k\sqrt{-1}},$$

ou, en réduisant les deux fractions au même dénominateur, de la forme

$$\frac{Px + Q}{(x - h)^2 + k^2}:$$

d'où il suit que la fraction $\frac{Px + Q}{(x-h)^2 + k^2}$, où P et Q désignent des constantes réelles, pourra remplacer, dans le développement de $\frac{F(x)}{f(x)}$, les deux fractions simples correspondantes aux racines $h \pm k\sqrt{-1}$.

Conditions pour que l'intégrale d'une différentielle rationnelle soit algébrique.

L'une des applications les plus importantes de la théorie qui vient d'être exposée, est l'intégration des différentielles rationnelles. Nous n'avons point à nous occuper ici des détails de cette intégration, et nous nous bornerons à donner les conditions pour qu'une différentielle rationnelle ait une intégrale algébrique.

Soit une différentielle rationnelle

$$\frac{F(x)}{f(x)}\,dx\,;$$

et

$$f(x) = (x-a)^{\alpha}(x-b)^{6}\ldots(x-c)^{\gamma},$$

$a, b, \ldots, c$ étant des quantités réelles ou imaginaires; on mettra la fraction $\frac{F(x)}{f(x)}$ sous la forme

$$\begin{aligned}\frac{F(x)}{f(x)} = E(x) &+ \frac{A}{(x-a)^{\alpha}} + \frac{A_1}{(x-a)^{\alpha-1}} + \ldots + \frac{A_{\alpha-1}}{x-a}\\ &+ \frac{B}{(x-b)^{6}} + \frac{B_1}{(x-b)^{6-1}} + \ldots + \frac{B_{6-1}}{x-b}\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ &+ \frac{C}{(x-c)^{\gamma}} + \frac{C_1}{(x-c)^{\gamma-1}} + \ldots + \frac{C_{\gamma-1}}{x-c}\end{aligned}$$

Pour avoir l'intégrale de $\frac{F(x)}{f(x)}dx$, il faut multiplier par dx chaque terme de cette valeur de $\frac{F(x)}{f(x)}$, et intégrer tous les résultats. Or les seuls parmi ces résultats dont l'intégrale n'est pas algébrique sont ceux qui ont pour dénominateur la première puissance de l'un des binômes $x-a$, $x-b$, etc.

On a en effet, si α' n'est pas égal à 1,

$$\int \frac{A\,dx}{(x-a)^{\alpha'}} = -\frac{A}{\alpha'(x-a)^{\alpha'-1}} + \text{constante},$$

et, si $\alpha'=1$,

$$\int \frac{A\,dx}{x-a} = A\log(x-a) + \text{constante}.$$

Donc, pour que $\frac{F(x)}{f(x)}dx$ ait une intégrale algébrique, il faut et il suffit que, dans le développement de $\frac{F(x)}{f(x)}$ en fractions simples, il n'y ait aucun terme dont le dénominateur soit du premier degré, c'est-à-dire que l'on ait

$$A_{\alpha-1}=0,\quad B_{\beta-1}=0,\ldots,\quad C_{\gamma-1}=0.$$

Cela exige d'abord que le polynôme $f(x)$ ne contienne aucun facteur linéaire simple.

Nous avons vu, dans la leçon précédente, qu'en posant

$$\varphi(x)=(x-a)^{\alpha}\frac{F(x)}{f(x)},\quad \psi(x)=(x-b)^{\beta}\frac{F(x)}{f(x)},\ldots,$$
$$\varpi(x)=(x-c)^{\gamma}\frac{F(x)}{f(x)},$$

on a

$$A_{\alpha-1}=\frac{\varphi^{\alpha-1}(a)}{1.2\ldots(\alpha-1)},\quad B_{\beta-1}=\frac{\psi^{\beta-1}(b)}{1.2\ldots(\beta-1)},\ldots,$$
$$C_{\gamma-1}=\frac{\varpi^{\gamma-1}(c)}{1.2\ldots(\gamma-1)};$$

les conditions pour que $\int \frac{F(x)}{f(x)}\,dx$ soit algébrique sont donc

$$\varphi^{\alpha-1}(a)=0,\quad \psi^{6-1}(b)=0,\ldots,\varpi^{\gamma-1}(c)=0,$$

quelles que soient les quantités a, $b,\ldots$, c, réelles ou imaginaires.

Ces conditions sont en même nombre que les racines a, $b,\ldots$, c; mais si le degré de $F(x)$ est inférieur de deux unités au moins à celui de $f(x)$, l'une d'elles sera comprise dans les autres. Désignons, en effet, par m le degré de $f(x)$, et supposons que $F(x)$ soit au plus du degré $m-2$; la partie entière $E(x)$ du développement de $\frac{F(x)}{f(x)}$ sera nulle, et, si l'on réduit au même dénominateur toutes les fractions de ce développement, pour les ajouter et recomposer la fraction $\frac{F(x)}{f(x)}$, on voit, sans peine, que le numérateur de la fraction ainsi obtenue contiendra x^{m-1} avec le coefficient

$$A_{\alpha-1}+B_{6-1}+\ldots+C_{\gamma-1}.$$

Ce coefficient doit être nul, puisque $F(x)$ est du degré $m-2$ au plus; on a donc

$$\frac{\varphi^{\alpha-1}(a)}{1.2\ldots(\alpha-1)}+\frac{\psi^{6-1}(b)}{1.2\ldots(6-1)}+\ldots+\frac{\varpi^{\gamma-1}(c)}{1.2\ldots(\gamma-1)}=0;$$

et, par conséquent, l'une des conditions pour que $\int \frac{F(x)}{f(x)}\,dx$ soit algébrique rentrera dans les autres.

L'équation précédente comprend, comme cas particulier, une formule démontrée dans la cinquième leçon, et sur laquelle nous avons eu occasion de nous appuyer.

J'indiquerai une seconde application importante de la

6

théorie des fractions rationnelles : elle est relative à la théorie des séries récurrentes.

Détermination du terme général d'une série récurrente.

Lorsqu'on divise deux polynômes $F(x)$ et $f(x)$ ordonnés par rapport aux puissances croissantes de x, et que l'opération ne se termine pas, le quotient forme une série dite *récurrente*, que l'on obtiendrait aussi en développant la fonction $\frac{F(x)}{f(x)}$ en série, par la formule de Maclaurin, ou par tout autre moyen; car on sait qu'une fonction n'est développable que d'une seule manière en série ordonnée suivant les puissances de la variable.

Voici le moyen le plus aisé, en général, de former cette série.

Décomposons la fraction $\frac{F(x)}{f(x)}$ en fractions simples, en adoptant le développement de la leçon précédente, et soit

$$\frac{F(x)}{f(x)} = E(x) + \sum \frac{A}{(x-a)^\alpha}$$

ce développement. Il n'y a plus maintenant qu'à développer en série, par la formule du binôme, chacune des fractions simples $\frac{A}{(x-a)^\alpha}$, ou $A(x-a)^{-\alpha}$. On a ainsi

$$(x-a)^{-\alpha} = (-a)^{-\alpha}\left(1-\frac{x}{a}\right)^{-\alpha}$$

$$= (-a)^{-\alpha}\left[\begin{array}{l} 1+\frac{\alpha}{1}\frac{x}{a}+\frac{\alpha(\alpha+1)}{1.2}\frac{x^2}{a^2}+\ldots \\ +\frac{\alpha(\alpha+1)\ldots(\alpha+n-1)}{1.2\ldots n}\frac{x^n}{a^n}+\ldots \end{array}\right];$$

et si ρ_n désigne le coefficient de x^n dans $E(x)$, le terme

général du développement de $\frac{F(x)}{f(x)}$ en série sera

$$x^n\left[\rho_n + \sum(-1)^\alpha \frac{\alpha(\alpha+1)\ldots(\alpha+n-1)}{1.2\ 3\ldots n}\frac{A}{a^{\alpha+n}}\right].$$

Dans le cas particulier où les racines a, etc., de $f(x)=0$ sont toutes simples, on a $\alpha = 1$ et $A = \frac{F(a)}{f'(a)}$; le terme général se réduit à

$$x^n\left[\rho_n - \sum\frac{F(a)}{a^{n+1}f'(a)}\right].$$

Ainsi la série récurrente dans laquelle se développe la fraction $\frac{F(x)}{f(x)}$ peut s'obtenir par l'addition de plusieurs séries provenant des développements de diverses puissances négatives et entières des binômes $a-x$, $b-x$, etc. D'ailleurs ces séries sont convergentes pour toutes les valeurs de x dont le module est inférieur au plus petit des modules des quantités a, b, etc.; d'où résulte ce théorème:

Théorème. — *Une série provenant du développement d'une fonction rationnelle* $\frac{F(x)}{f(x)}$ *est convergente pour toutes les valeurs réelles ou imaginaires de* x *dont le module est inférieur au plus petit module des racines de l'équation* $f(x)=0$.

Ce théorème a été généralisé par M. Cauchy et étendu à toutes les fonctions; on trouvera tous les développements que comporte cette importante question dans les *Exercices de Mathématiques* de M. Cauchy et dans le *Journal de Mathématiques* de M. Liouville.

Nous terminerons cette leçon par une application de la méthode qui vient d'être indiquée.

Exemple. — Proposons-nous de former la série récur-

rente dans laquelle se développe la fonction

$$\varphi(x) = \frac{P + Qx}{1 - 2x\cos\omega + x^2},$$

où P, Q et ω désignent des constantes données.

Décomposant cette fraction en fractions simples, et employant, pour abréger l'écriture, la notation usuelle des exponentielles imaginaires, savoir,

$$e^{\pm\omega\sqrt{-1}} = \cos\omega \pm \sqrt{-1}\sin\omega,$$

on a

$$\varphi(x) = \frac{A}{1 - xe^{\omega\sqrt{-1}}} - \frac{B}{1 - xe^{-\omega\sqrt{-1}}},$$

A et B étant des constantes qui ont respectivement pour valeurs

$$A = \frac{Pe^{\omega\sqrt{-1}} + Q}{2\sin\omega\sqrt{-1}}, \quad B = \frac{Pe^{-\omega\sqrt{-1}} + Q}{2\sin\omega\sqrt{-1}}.$$

Développant en série chacune des parties de $\varphi(x)$, on trouve

$$\varphi(x) = A\sum x^n e^{n\omega\sqrt{-1}} - B\sum x^n e^{-n\omega\sqrt{-1}},$$

ou, en remplaçant A et B par leurs valeurs,

$$\varphi(x) = \sum \frac{\left(Pe^{\omega\sqrt{-1}} + Q\right)e^{n\omega\sqrt{-1}} - \left(Pe^{-\omega\sqrt{-1}} + Q\right)e^{-n\omega\sqrt{-1}}}{2\sin\omega\sqrt{-1}}\, x^n.$$

En remettant à la place des exponentielles imaginaires leurs valeurs, on a, toutes réductions faites,

$$\frac{P + Qx}{1 - 2x\cos\omega + x^2} = \sum \frac{P\sin(n+1)\omega + Q\sin n\omega}{\sin\omega}\, x^n.$$

Le terme général du développement est donc

$$\left(P\frac{\sin(n+1)\omega}{\sin\omega} + Q\frac{\sin n\omega}{\sin\omega}\right) x^n.$$

HUITIÈME LEÇON.

Des fonctions symétriques et rationnelles des solutions communes à deux ou plusieurs équations. — Extension de la méthode d'élimination par les fonctions symétriques, au cas d'un nombre quelconque d'équations. — Théorème de Bezout sur le degré de l'équation finale. — Méthode de Tschirnaüs, pour faire disparaître autant de termes que l'on veut d'une équation. — Application au troisième et au quatrième degré.

Nous avons exposé dans la troisième leçon une méthode fondée sur la théorie des fonctions symétriques, pour l'élimination d'une inconnue entre deux équations, et nous en avons déduit que le degré de l'équation finale est, au plus, égal au produit des degrés des deux équations données. Bezout a généralisé cette proposition en démontrant que *le degré de l'équation finale résultant de l'élimination de $k-1$ inconnues entre k équations est, au plus, égal au produit des degrés de ces équations.* Pour établir ce théorème, nous suivrons la marche indiquée par Poisson dans le onzième cahier du *Journal de l'École Polytechnique*. Nous commencerons par étendre au cas d'un nombre quelconque d'équations la méthode d'élimination par les fonctions symétriques, précédemment exposée pour le cas de deux équations seulement. Cette extension repose sur la considération des fonctions symétriques des solutions communes à plusieurs équations, dont nous allons d'abord nous occuper.

Pour éviter les difficultés que peuvent présenter quelques cas particuliers, je préviens, une fois pour toutes, que nous raisonnerons toujours, dans cette leçon, sur des

équations générales dont les coefficients demeurent indéterminés.

Toutes les conséquences auxquelles nous serons conduit, auront lieu en général, si l'on attribue aux coefficients des valeurs déterminées; mais nos raisonnements pourront être en défaut dans quelques cas particuliers.

Des fonctions symétriques des solutions communes à deux ou plusieurs équations.

Cas de deux équations. — Soient deux équations

$$f(x, y) = 0, \quad F(x, y) = 0,$$

entre les deux inconnues x et y, et

$$(x_1 y_1), \quad (x_2 y_2), \ldots, \quad (x_n y_n)$$

les couples de solutions communes à ces deux équations. On nomme *fonctions symétriques de ces solutions communes* toute fonction qui ne change pas de valeur, quand on y permute les groupes $(x_1 y_1)$, $(x_2 y_2)$, etc., les uns dans les autres; mais nous considérerons seulement les fonctions symétriques rationnelles. Une fonction de cette espèce, de même que les fonctions symétriques des racines d'une équation à une inconnue, est exprimable rationnellement par les coefficients des équations proposées.

Par un raisonnement tout semblable à celui que nous avons fait sur les fonctions symétriques des racines d'une équation, on fera voir que la détermination d'une fonction rationnelle et symétrique des solutions $(x_1 y_1)$, $(x_2 y_2)$, etc., se ramène à celle de fonctions symétriques entières, homogènes, et dont les différents termes se déduisent les uns des autres, en changeant les indices des lettres x et y, mais sans changer leurs exposants. Les fonctions symétriques auxquelles on est ainsi ramené seront dites *simples* ou du

premier ordre, *doubles* ou du deuxième ordre, etc., suivant que chacun de leurs termes contiendra les lettres d'un, de deux, etc., groupes $(x_1 y_1)$, $(x_2 y_2)$, etc. La forme générale des fonctions simples sera

$$x_1^p y_1^q + x_2^p y_2^q + \ldots + x_n^p y_n^q,$$

p ou q pouvant être nul. Nous représenterons une pareille fonction par $\sum x_1^p\ y_1^q$. La forme des fonctions doubles sera

$$x_1^p y_1^q x_2^{p'} y_2^{q'} + x_1^p\ y_1^q\ x_3^{p'} y_3^{q'} + \ldots.$$

Nous la représenterons par $\sum x_1^p\ y_1^q\ x_2^{p'} y_2^{q'}$, et ainsi de suite.

Waring est le premier qui ait considéré les fonctions symétriques de cette espèce. Il a indiqué, dans ses *Meditationes algebraicæ*, un moyen qui s'offre naturellement, mais qui est presque impraticable, pour calculer la fonction simple $\sum x_1^p y_1^q$. Ce moyen consiste à éliminer x et y entre les équations proposées et l'équation

$$t = x^p y^q;$$

l'équation finale en t ayant pour racines

$$x_1^p\ y_1^q,\quad x_2^p\ y_2^q, \ldots,\quad x_n^p\ y_n^q,$$

la fonction simple $\sum x_1^p y_1^q$ sera égale au coefficient du second terme pris en signe contraire. Sans insister sur les inconvénients que présente un pareil procédé, nous exposerons immédiatement la méthode imaginée par Poisson.

Désignons par t une nouvelle variable, par α une in-

déterminée, et posons

$$t = x + \alpha y, \quad \text{d'où} \quad x = t - \alpha y;$$

en substituant cette valeur de x dans les équations proposées, celles-ci deviennent

$$f(t - \alpha y, y) = 0, \quad F(t - \alpha y, y) = 0,$$

et, en éliminant y, on aura une équation finale en t

$$\psi(t, \alpha) = 0,$$

qui contient dans ses différents termes l'indéterminée α. Cette équation en t aura pour racines

$$x_1 + \alpha y_1, \quad x_2 + \alpha y_2, \ldots, \quad x_n + \alpha y_n,$$

et sera, par conséquent, du degré n. D'ailleurs la somme des puissances semblables de degré μ des racines de l'équation en t peut s'exprimer rationnellement (première leçon) par les coefficients de cette équation, c'est-à-dire en fonction de α et des coefficients des équations proposées. On aura donc

$$(x_1 + \alpha y_1)^\mu + (x_2 + \alpha y_2)^\mu + \ldots + (x_n + \alpha y_n)^\mu$$
$$= A_0 + A_1 \alpha + A_2 \alpha^2 + \ldots,$$

où A_0, A_1, etc., désignent des quantités connues et exprimées rationnellement par les coefficients des équations proposées. Cette équation ayant lieu quelle que soit α, les coefficients des mêmes puissances de α doivent être égaux dans les deux membres; d'où résulte cette suite d'égalités :

$$x_1^\mu + x_2^\mu + \ldots + x_n^\mu = A_0,$$

$$\frac{\mu}{1}\left(x_1^{\mu-1} y_1 + x_2^{\mu-1} y_2 + \ldots + x_n^{\mu-1} y_n\right) = A_1,$$

$$\frac{\mu(\mu-1)}{1.2}\left(x_1^{\mu-2} y_1^2 + x_2^{\mu-2} y_2^2 + \ldots + x_n^{\mu-2} y_n^2\right) = A_2,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$y_1^\mu + y_2^\mu + \ldots + y_n^\mu = A_\mu,$$

qui feront connaître les fonctions simples $\sum x_1^p\, y_1^q$ de degré $p+q=\mu$.

Le calcul des fonctions doubles, triples, etc., se fait de la même manière que pour les fonctions symétriques ordinaires. Par exemple, pour avoir la fonction double $\sum x_1^p\, y_1^q\, x_2^{p'}\, y_2^{q'}$, on multiplicra ensemble les deux fonctions simples $\sum x_1^p\, y_1^q$ et $\sum x_1^{p'}\, y_1^{q'}$; le produit se composera de la fonction simple $\sum x_1^{p+p'}\, y_1^{q+q'}$ et de la fonction double qu'on veut trouver. On aura donc

$$\sum x_1^p\, y_1^q\, x_2^{p'}\, p_2^{q'} = \sum x_1^p\, y_1^q \sum x_1^{p'}\, y_1^{q'} - \sum x_1^{p+p'}\, y_1^{q+q'}.$$

Seulement, il faudrait ne prendre que la moitié de cette valeur, si l'on avait à la fois $p'=p$, $q'=q$.

Les fonctions triples, etc., se calculeront d'une manière analogue.

Ce qui précède suffit pour établir, comme nous l'avions annoncé, que les fonctions symétriques et rationnelles des solutions communes à deux équations peuvent s'exprimer rationnellement par les coefficients de ces équations, et l'on voit que leur détermination n'exige que l'élimination d'une inconnue entre deux équations.

Cas d'un nombre quelconque d'équations. — La même méthode s'applique à un nombre quelconque d'équations. Supposons qu'il s'agisse de trois équations à trois inconnues

$$f(x, y, z) = 0, \quad F(x, y, z) = 0, \quad \varphi(x, y, z) = 0,$$

et soient

$$(x_1, y_1, z_1), \quad (x_2, y_2, z_2), \ldots, \quad (x_n, y_n, z_n)$$

les groupes de solutions communes à ces trois équations.

Conservant la classification que nous avons adoptée des diverses fonctions symétriques, la forme générale des fonctions simples sera

$$x_1^p y_1^q z_1^r + x_2^p y_2^q z_2^r + \ldots + x_n^p y_n^q z_n^r,$$

celle des fonctions doubles sera

$$x_1^p y_1^q z_1^r x_2^{p'} y_2^{q'} z_2^{r'} + \ldots,$$

et ainsi de suite. Et c'est à la détermination des premières que se ramène celle de la fonction symétrique et rationnelle la plus compliquée.

Désignant par t une nouvelle variable, par α et 6 deux indéterminées, nous poserons

$$t = x + \alpha y + 6z, \quad \text{d'où} \quad x = t - \alpha y - 6z.$$

Ayant substitué cette valeur de x dans les équations proposées, nous éliminerons y et z; nous obtiendrons ainsi une équation finale en t,

$$\psi(t, \alpha, 6) = 0,$$

contenant les indéterminées α et 6, et dont les racines seront

$$x_1 + \alpha y_1 + 6z_1, \quad x_2 + \alpha y_2 + 6z_2, \ldots, \quad x_n + \alpha y_n + 6z_n.$$

La somme des puissances μ de ces racines pourra s'exprimer rationnellement par les coefficients de l'équation en t, c'est-à-dire en fonction des indéterminées α et 6, et des coefficients des équations proposées. On aura ainsi une équation de la forme

$$\sum (x_1 + \alpha y_1 + 6z_1)^\mu = \sum A_{q,r}\, \alpha^q 6^r,$$

où le coefficient $A_{q,r}$ désigne généralement une quantité connue. Le signe Σ du premier membre s'étend aux n racines de l'équation en t, celui du second membre à

toutes les valeurs de q et de r, telles que

$$q + r = \quad \text{ou} \quad < \mu.$$

En posant $p = \mu - q - r$, et égalant les coefficients de $\alpha^q \, 6^r$ dans les deux membres, on aura

$$\frac{1.2.3\ldots\mu}{(1.2\ldots p)(1.2\ldots q)(1.2\ldots r)} \sum x_1^p y_1^q z_1^r = \mathrm{A}_{q,r};$$

c'est la formule qui fera connaître les fonctions simples.

Pour former les fonctions doubles, triples, etc., on procédera comme dans le cas de deux équations. La forme du calcul est la même, et l'on voit qu'en général les fonctions symétriques et rationnelles des solutions communes à plusieurs équations s'exprimeront toujours rationnellement par les coefficients de ces équations.

Remarque. — La détermination des fonctions symétriques des solutions communes à trois équations exige l'élimination de deux inconnues entre trois équations, et généralement la détermination des fonctions symétriques des solutions communes à k équations exige l'élimination de $k-1$ inconnues entre k équations.

Extension de la méthode d'élimination par les fonctions symétriques, au cas d'un nombre quelconque d'équations.

La méthode que nous allons exposer, d'après Poisson, donne le moyen d'éliminer $k-1$ inconnues entre k équations, lorsqu'on sait éliminer $k-2$ inconnues entre $k-1$ équations, et, par conséquent, ramène tous les cas, en dernière analyse, à l'élimination d'une inconnue entre deux équations.

Pour fixer les idées, nous considérerons quatre équations seulement, entre quatre ou un plus grand nombre d'inconnues; mais on verra sans peine que notre raison-

nement est général et s'appliquerait sans modification au cas d'un nombre quelconque d'équations.

Soient donc les quatre équations

$$(1)\quad \begin{cases} f(x, y, z, u, \ldots) = 0, \\ F(x, y, z, u, \ldots) = 0, \\ \varphi(x, y, z, u, \ldots) = 0, \\ \Phi(x, y, z, u, \ldots) = 0, \end{cases}$$

entre quatre ou un plus grand nombre d'inconnues x, y, z, u, etc., et proposons-nous d'éliminer trois inconnues, x, y, z par exemple, entre ces quatre équations.

Considérons en particulier les trois premières des équations (1),

$$(2)\quad \begin{cases} f(x, y, z, u, \ldots) = 0, \\ F(x, y, z, u, \ldots) = 0, \\ \varphi(x, y, z, u, \ldots) = 0, \end{cases}$$

et, regardant x, y, z comme fonctions des autres variables u, etc., désignons par

$$(x_1, y_1, z_1), \quad (x_2, y_2, z_2), \ldots, \quad (x_n, y_n, z_n)$$

les n systèmes de solutions communes aux équations (2).

Cela posé, remplaçons (x, y, z), dans la quatrième des équations (1), successivement par chacun de ces n systèmes, et désignons par V le produit des résultats ainsi obtenus, en sorte qu'on ait

$$(3)\quad V = \Phi(x_1, y_1, z_1, u, \ldots)\,\Phi(x_2, y_2, z_2, u, \ldots)\ldots\Phi(x_n, y_n, z_n, u, \ldots);$$

l'équation

$$(4)\qquad V = 0$$

sera l'équation finale résultant de l'élimination de x, y et z entre les équations (1), car cette équation (4) exprime la condition nécessaire et suffisante pour que les équa-

tions (1) admettent un système de solutions communes pour x, y et z. D'ailleurs V est une fonction symétrique et entière des solutions communes aux équations (2); on pourra donc l'exprimer rationnellement par les quantités indépendantes de x, y, z qui entrent dans les équations (1). Pour cela, désignant, comme précédemment, par t une nouvelle variable, par α et 6 deux paramètres indéterminés, nous poserons

$$t = x + \alpha y + 6z, \quad \text{d'où} \quad x = t - \alpha y - 6z;$$

en substituant cette valeur de x dans les équations (2), on aura les trois suivantes :

$$(5) \quad \begin{cases} f(t - \alpha y - 6z, y, z, u, \ldots) = 0, \\ F(t - \alpha y - 6z, y, z, u, \ldots) = 0, \\ \varphi(t - \alpha y - 6z, y, z, u, \ldots) = 0, \end{cases}$$

entre lesquelles il faudra éliminer y et z. C'est donc à l'élimination de deux inconnues entre trois équations que nous ramenons l'élimination de trois inconnues entre quatre équations. L'équation finale en t qui résulte de l'élimination de y et z entre les équations (5) aura pour racines

$$x_1 + \alpha y_1 + 6z_1, \quad x_2 + \alpha y_2 + 6z_2, \ldots, x_n + \alpha y_n + 6z_n,$$

et sera, par conséquent, du degré n. Supposons-la formée, et ordonnons-la par rapport à t; elle sera

$$(6) \quad t^n + p_1 t^{n-1} + p_2 t^{n-2} + \ldots + p_{n-1} t + p_n = 0,$$

p_1, p_2, etc., étant des fonctions rationnelles de u, etc., qui contiennent aussi les paramètres α et 6. Cette équation (6) servira, comme nous l'avons vu précédemment, à calculer les diverses fonctions symétriques des solutions communes aux équations (2), dont l'expression de V est composée, et le problème sera enfin résolu.

Cette méthode conduirait, dans les applications, à des calculs d'une longueur rebutante; mais l'objet principal que nous avons en vue est d'en déduire le théorème de Bezout, relatif au degré de l'équation finale.

Théorème de Bezout sur le degré de l'équation finale.

D'après ce qui précède, n étant le nombre des solutions communes (x, y, z) aux équations (2), on obtiendra une équation finale du même degré n en éliminant deux inconnues quelconques entre les équations (2). Cela est d'ailleurs évident à priori; car, à cause de la généralité que nous supposons aux équations, tout est semblable par rapport à x, y, z, u, etc. Toutefois il est important de faire cette remarque, parce que le contraire pourrait avoir lieu si l'on attribuait aux coefficients des valeurs particulières.

Lemme. — *Si n désigne le degré de l'équation finale résultant de l'élimination de deux inconnues entre les trois premières des équations* (1), *et m le degré de la quatrième équation* (1), *le degré de l'équation finale résultant de l'élimination de trois inconnues entre les quatre équations* (1) *est au plus égal à mn.*

L'équation (6), qui résulte de l'élimination de y et z entre les équations (5), étant du degré n, les coefficients p_1, p_2, etc., seront des fonctions entières de u, etc., dont la première sera au plus du premier degré, la deuxième du second, etc. Cela posé, la somme des puissances semblables de degré μ des racines de l'équation (6), c'est-à-dire $\sum(x_1 + \alpha y_1 + 6 z_1)^{\mu}$, s'exprimera sous forme entière, en fonction des coefficients p_1, p_2, etc., par une formule qui sera au plus du degré μ par rapport à u, etc. (*voir* première leçon); donc, une fonction symétrique

simple, telle que $\sum x_1^p y_1^q z_1^r$, de degré $p+q+r=\mu$, s'exprimera par une formule qui sera elle-même au plus de ce degré μ, par rapport à u, etc. Il résulte de là, et du mode général suivant lequel les fonctions symétriques et entières les plus compliquées se forment à l'aide des fonctions simples, que toute fonction symétrique et entière de degré μ des solutions communes (x_1, y_1, z_1), etc., aux équations (2), s'exprimera par une formule entière qui sera au plus du degré μ par rapport à u, etc. Or les différents termes de l'expression de V, donnée par l'équation (3), sont le produit de puissances de u, etc., dont les exposants ont une somme $mn-\mu$ inférieure à mn, par une fonction symétrique entière de degré μ des solutions communes (x_1, y_1, z_1), etc., aux équations (2). Donc enfin, chacune de ces parties de V s'exprimera par une formule au plus du degré mn par rapport à u, etc., et, par suite, l'équation $V=0$ sera au plus du degré mn.

Remarque. — On pourrait faire à la démonstration précédente l'objection que voici : Le raisonnement suppose que les coefficients p_1, p_2, etc., sont entiers par rapport aux variables u, etc., ou, en d'autres termes, que l'équation (6), qui est du degré n par rapport à chacune des variables t, u, etc., soit de ce même degré par rapport à toutes les variables. Or cela n'est pas tout à fait évident, quoique les équations (1) ou (5) soient supposées chacune la plus générale de son degré. Voici, ce me semble, la manière la plus simple de lever cette objection. Si quelques-uns des coefficients p_1, p_2, etc., étaient fractionnaires, quelques-unes des racines t de l'équation (6) deviendraient infinies pour certaines valeurs finies des variables u, etc. Or je dis que cela ne peut avoir lieu, tant qu'on laisse indéterminés les coefficients des équations (2) ou (5), et il suffit évidemment, pour justifier cette assertion, de citer un

cas où cela ne soit pas. Supposons qu'on donne aux coefficients des équations (5) des valeurs telles, que chacune, restant du même degré, se décompose en facteurs linéaires de la forme $t + ay + bz + cu + \ldots + l$: on pourra exprimer chacune des racines t de l'équation finale relative à ces équations particulières, en fonction de u, etc., par les formules qui servent à la résolution des équations du premier degré; et ces valeurs de t, étant évidemment de la forme $gu + \ldots + f$, ne pourront devenir infinies pour des valeurs finies de u, etc.

On déduit aisément du lemme qui précède la démonstration du théorème de Bezout.

Théorème. — *Le degré de l'équation finale résultant de l'élimination de $k - 1$ inconnues entre k équations est égal au produit des degrés de ces équations.*

Soient, en effet,

$$m_1, \ m_2, \ m_3, \ldots, \ m_k$$

les degrés de k équations. Le degré de l'équation finale résultant de l'élimination d'une inconnue entre les deux premières sera égal à m_1, m_2, ainsi que nous l'avons établi dans la troisième leçon : donc, d'après le lemme qui précède, si l'on élimine deux inconnues entre les trois premières, le degré de l'équation finale sera au plus $m_1 m_2 \times m_3$, ou $m_1 m_2 m_3$; de même, si l'on élimine trois inconnues entre les quatre premières, le degré de l'équation finale sera au plus $m_1 m_2 m_3 \times m_4$ ou $m_1 m_2 m_3 m_4$. Et l'on voit, en continuant ainsi, que le degré de l'équation finale résultant de l'élimination de $k - 1$ inconnues entre les k équations sera au plus égal au produit des degrés de ces équations.

On peut même ajouter que le degré de l'équation finale sera précisément égal à ce produit, si les équations proposées sont chacune la plus générale de son degré, comme

nous l'avons supposé. On s'en assurera aisément en considérant un système de k équations décomposables chacune en facteurs linéaires, ainsi que nous l'avons fait dans la troisième leçon, pour le cas de deux équations.

Corollaire. — Il résulte du théorème précédent et des développements exposés dans la quatrième leçon, que la résolution de plusieurs équations simultanées peut se ramener à la résolution d'une seule équation dont le degré est généralement égal au produit des degrés des proposées.

Méthode de Tschirnaüs, pour faire disparaître autant de termes que l'on veut d'une équation.

Tschirnaüs a donné, dans les *Actes de Leipsick* pour 1683, une méthode élégante, qui sert à faire disparaître d'une équation autant de termes que l'on veut. Cette méthode consiste à transformer l'équation proposée en une autre dont la racine soit une fonction rationnelle de celle de la proposée, ou, si l'on veut, une fonction entière de degré inférieur à celui de l'équation proposée, car c'est à cette forme que peut se ramener la fonction rationnelle la plus générale (deuxième leçon).

Soit

$$(1) \qquad x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0$$

une équation du degré m, et posons

$$(2) \qquad y = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} + x^n,$$

a_0, a_1, etc., désignant des indéterminées, et n un entier inférieur à m. L'équation finale en y, résultant de l'élimination de x entre les équations (1) et (2), sera évidemment du degré m, puisque y a autant de valeurs que x. Cette élimination peut se faire par les fonctions symétriques, de la manière suivante : En élevant l'équation (2) aux différentes puissances 2, 3, ..., m, et ayant soin de

rabaisser les exposants de x au-dessous de m, à l'aide de l'équation (1), on aura une suite d'équations de la forme

$$(3)\quad \begin{cases} y^2 = b_0 + b_1 x + b_2 x^2 + \ldots + b_{m-1} x^{m-1}, \\ y^3 = c_0 + c_1 x + \ldots\ldots\ldots + c_{m-1} x^{m-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ y^m = k_0 + k_1 x + \ldots\ldots\ldots + k_{m-1} x^{m-1}, \end{cases}$$

b_0, b_1, etc., étant des fonctions des indéterminées a_0, a_1, etc. Si, maintenant, s_1, s_2, etc., désignent les sommes de puissances semblables des racines de l'équation (1), S_1, S_2, etc., celles des puissances semblables des racines de l'équation en y, les équations (2) et (3) donneront

$$(4)\quad \begin{cases} S_1 = m a_0 + a_1 s_1 + a_2 s_2 + \ldots + a_{n-1} s_{n-1} + s_n, \\ S_2 = m b_0 + b_1 s_1 + b_2 s_2 + \ldots + b_{m-1} s_{m-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ S_m = m k_0 + k_1 s_1 + k_2 s_2 + \ldots + k_{m-1} s_{m-1}. \end{cases}$$

Connaissant ainsi les sommes de puissances semblables des racines de l'équation en y, on formera aisément cette équation.

On peut y arriver encore de la manière suivante. On résoudra les équations (3) par rapport aux puissances $x^1, x^2, \ldots, x^{m-1}$, et l'on portera leurs valeurs dans l'équation (2). Ce procédé a l'avantage de donner la valeur de x exprimée rationnellement en y, en sorte qu'on connaîtra chaque racine de l'équation proposée, quand on aura résolu l'équation finale en y.

Représentons par

$$(5)\quad y^m + q_1 y^{m-1} + q_2 y^{m-2} + \ldots + q_{m-1} y + q_m = 0$$

cette équation en y, où $q_1, q_2, \ldots, q_m$ sont fonctions des indéterminées a_0, a_1, etc., et qui exprime la condition

pour que les équations (1) et (2) aient une racine commune. Je dis que de cette seule équation (5) on peut déduire la valeur de x qui correspond à chaque valeur de y, et même la valeur d'une puissance quelconque de x. En effet, y est une fonction des indéterminées a_0, a_1, etc., considérées comme des variables indépendantes, et l'on a alors

$$\frac{dy}{da_1} = x, \quad \frac{dy}{da_2} = x^2, \ldots$$

Différentions maintenant l'équation (5) par rapport à a_1, dont y, q_1, q_2, etc., sont fonctions; on aura

$$[my^{m-1} + (m-1) q_1 y^{m-2} + \ldots + q_{m-1}] \frac{dy}{da_1}$$
$$+ \left(y^{m-1} \frac{dq_1}{da_1} + y^{m-2} \frac{dq_2}{da_1} + \ldots + \frac{dq_m}{da_1} \right) = 0,$$

et, par suite,

$$x = -\frac{y^{m-1} \frac{dq_1}{da_1} + y^{m-2} \frac{dq_2}{da_1} + \ldots + \frac{dq_m}{da_1}}{my^{m-1} + (m-1) q_1 y^{m-2} + \ldots + q_{m-1}}.$$

On trouverait de même, en différentiant, l'équation (5) par rapport à a_2,

$$x^2 = -\frac{y^{m-1} \frac{dq_1}{da_2} + y^{m-2} \frac{dq_2}{da_2} + \ldots + \frac{dq_m}{da_2}}{my^{m-1} + (m-1) q_1 y^{m-2} + \ldots + q^{m-1}},$$

et ainsi de suite; mais ces diverses valeurs sont seulement curieuses, car elles n'ont pas la forme la plus simple qu'on puisse leur donner.

On voit, par ce qui précède, qu'il suffira de résoudre l'équation (5) pour avoir résolu par cela même l'équation (1).

Cela posé, on peut disposer des n indéterminées a_0, a_1, etc., de manière à faire évanouir n termes de l'équation en y, à partir du second par exemple. Il faudra alors,

d'après les formules de Newton, que l'on ait

$$S_1 = 0, \quad S_2 = 0, \ldots, \quad S_n = 0.$$

Or, en se reportant aux équations (4), on voit que S_1 est du premier degré par rapport à a_0, a_1, etc., que S_2 est du deuxième, S_3 du troisième, etc., S_n du $n^{ième}$. Donc, d'après le théorème de Bezout, la détermination de ces indéterminées dépend d'une équation du degré

$$1.2.3\ldots n,$$

et, si l'on voulait faire disparaître de l'équation (5) tous les termes, à l'exception du premier et du dernier, le problème dépendrait du degré

$$1.2.3\ldots(m-1).$$

C'est aussi à la résolution d'une équation de ce degré que se trouverait ramenée celle de l'équation proposée, car l'équation (5) n'ayant alors que deux termes serait immédiatement résolue.

Application au troisième et au quatrième degré.

Nous reviendrons, dans une prochaine leçon, sur la résolution des équations générales du troisième et du quatrième degré; mais nous ferons voir immédiatement comment résulte de la transformation de Tschirnaüs la possibilité d'effectuer cette résolution.

Soit d'abord l'équation du troisième degré

$$x^3 + px^2 + qx + s = 0;$$

on posera

$$y = a + bx + x^2,$$

et l'on formera l'équation finale en y, savoir

$$y^3 + Py^2 + Qy + R = 0.$$

On déterminera a et b à l'aide des équations $P = 0$, $Q = 0$,

qui sont, l'une du premier degré, l'autre du second; on pourra donc les résoudre et exprimer a et b en fonction des coefficients de la proposée. L'équation en y se réduisant alors à

$$y^3 + R = 0,$$

on en tirera ces trois valeurs

$$y = \sqrt[3]{-R}, \quad y = \alpha\sqrt[3]{-R}, \quad y = 6\sqrt[3]{-R},$$

α et 6 désignant les racines cubiques imaginaires de 1. Connaissant ainsi les trois valeurs de y, on aura facilement, par ce que nous avons dit plus haut, les trois valeurs de x.

Soit enfin l'équation du quatrième degré

$$x^4 + px^3 + qx^2 + rx + s = 0;$$

on posera, comme précédemment,

$$y = a + bx + x^2,$$

et l'on aura une équation en y telle, que

$$y^4 + Py^3 + Qy^2 + Ry + S = 0.$$

On déterminera a et b à l'aide des équations $P = 0$, $R = 0$, qui sont, l'une du premier degré, l'autre du troisième; on pourra donc les résoudre et exprimer a et b en fonction des coefficients de la proposée. L'équation en y, se réduisant à

$$y^4 + Qy^2 + S = 0,$$

pourra elle-même être résolue, puisqu'elle est bicarrée. Connaissant les quatre valeurs de y, on aura aussi les quatre racines de l'équation proposée.

NEUVIÈME LEÇON.

Développement d'une fonction algébrique implicite, en série ordonnée suivant les puissances décroissantes de sa variable. — Formation de l'équation finale résultant de l'élimination d'une inconnue entre deux équations à deux inconnues. Nouvelle démonstration du théorème de Bezout. Somme des racines de l'équation finale. — Nouvelle démonstration d'une formule d'analyse. — Démonstration d'un théorème de géométrie.

Les recherches que je vais exposer dans cette leçon font partie d'un beau Mémoire sur l'élimination, publié par M. Liouville, dans le tome VI de son *Journal de Mathématiques*.

Développement d'une fonction algébrique implicite, en série ordonnée suivant les puissances décroissantes de sa variable.

Soit

$$(1) \qquad M(x, y) = 0, \quad \text{ou} \quad M = 0,$$

une équation du degré m entre deux variables x et y. Si cette équation est du degré m par rapport à y, elle aura m racines y, qui seront fonctions de x, et que nous nous proposons de développer suivant les puissances décroissantes de x. En réunissant les termes de même degré, l'équation (1) pourra s'écrire de la manière suivante :

$$(2) \qquad x^m f\left(\frac{y}{x}\right) + x^{m-1} f_1\left(\frac{y}{x}\right) + x^{m-2} f_2\left(\frac{y}{x}\right) + \ldots = 0,$$

ou, en posant $\frac{y}{x} = u$,

$$(3) \qquad x^m f(u) + x^{m-1} f_1(u) + x^{m-2} f_2(u) + \ldots = 0;$$

f, f_1, f_2, etc., désignent ici des polynômes dont le premier est du degré m, et les autres au plus des degrés $m-1$, $m-2$, etc., respectivement. Dans le cas le plus général, ces polynômes seront précisément des degrés m, $m-1$, $m-2$, etc.

Les m valeurs de u fournies par l'équation (3) sont des fonctions de x, qui, pour $x=\infty$, se réduiront aux m racines de l'équation

$$(4) \qquad f(\alpha)=0;$$

on pourra donc poser généralement

$$(5) \qquad u=\alpha+\varepsilon,$$

ε s'annulant avec $\frac{1}{x}$. La méthode des asymptotes donne le moyen de calculer la limite du produit εx. Nous nous bornerons au cas où les racines de l'équation (4) sont inégales, et dans tout ce qui suit, cette hypothèse doit être maintenue. Portons dans l'équation (3) la valeur de u tirée de (5); on aura

$$(6) \quad x^m f(\alpha+\varepsilon)+x^{m-1}f_1(\alpha+\varepsilon)+x^{m-2}f_2(\alpha+\varepsilon)+\ldots=0.$$

Développant chaque terme par la formule de Taylor, ayant égard à l'équation (4), et divisant par x^{m-1}, il vient

$$(7) \quad \left\{ \begin{array}{l} [(\varepsilon x)f'(\alpha)+f_1(\alpha)] \\ +\frac{1}{x}\left[\frac{(\varepsilon x)^2}{1.2}f''(\alpha)+(\varepsilon x)f'_1(\alpha)+f_2(\alpha)\right]+\ldots=0; \end{array} \right.$$

faisant maintenant $x=\infty$ dans cette équation, et désignant par α' la limite de εx, il vient

$$(8) \qquad \alpha' f'(\alpha)+f_1(\alpha)=0,$$

d'où

$$(9) \qquad \alpha'=-\frac{f_1(\alpha)}{f'(\alpha)}.$$

Cette valeur de α' sera toujours finie, car, par hypothèse, $f(\alpha)$ n'a pas de racines égales.

Puisque εx a pour limite la quantité α', dont nous venons de trouver la valeur, on pourra poser

$$\varepsilon x = \alpha' + \varepsilon',$$

d'où

$$\varepsilon = \frac{\alpha'}{x} + \frac{\varepsilon'}{x}, \tag{10}$$

ε' s'annulant avec $\frac{1}{x}$. Par suite, la valeur (5) de u devient

$$u = \alpha + \frac{\alpha'}{x} + \frac{\varepsilon'}{x}. \tag{11}$$

C'est la série dans laquelle u se développe, quand on se borne aux deux premiers termes; $\frac{\varepsilon'}{x}$ est le reste correspondant.

On peut déterminer la limite du produit $\varepsilon' x$ de la même manière que celle du produit εx. Si, en effet, on porte dans l'équation (7) la valeur de ε, tirée de (10), qu'on multiplie ensuite par x, et qu'on ait égard à l'équation (8), il vient

$$(\varepsilon' x) f'(\alpha) + \left[\frac{\alpha'^2}{1.2} f''(\alpha) + \alpha' f_1'(\alpha) + f_2(\alpha)\right] + \text{E} = 0,$$

en désignant par E une somme de termes qui s'annulent avec $\frac{1}{x}$; faisant donc $x = \infty$, et désignant par α'' la limite de $\varepsilon' x$, on a

$$\alpha'' f'(\alpha) + \left[\frac{\alpha'^2}{1.2} f''(\alpha) + \alpha' f_1'(\alpha) + f_2(\alpha)\right] = 0, \tag{12}$$

équation qui détermine la valeur de α''.

Connaissant la limite α'' du produit $\varepsilon' x$, on pourra poser

$$\varepsilon' x = \alpha'' + \varepsilon'';$$

d'où

(13) $$\varepsilon' = \frac{\alpha''}{x} + \frac{\varepsilon''}{x},$$

ε'' étant une nouvelle quantité qui s'évanouit avec $\frac{1}{x}$. D'après cela, la valeur (11) de u devient

(14) $$u = \alpha + \frac{\alpha'}{x} + \frac{\alpha''}{x^2} + \frac{\varepsilon''}{x^2}.$$

C'est la série qui exprime la valeur de u quand on se borne aux trois premiers termes; $\frac{\varepsilon''}{x^2}$ est le reste correspondant.

On pourrait obtenir ainsi autant de termes que l'on voudrait du développement de u, et comme $y = ux$, on aura, par suite, autant de termes que l'on voudra du développement de y; on a, en particulier,

(15) $$\left\{\begin{array}{l} y = \alpha x + \varepsilon x, \\ y = \alpha x + \alpha' + \varepsilon', \\ y = \alpha x + \alpha' + \dfrac{\alpha''}{x} + \dfrac{\varepsilon''}{x}. \end{array}\right.$$

La seconde de ces trois formules comprend toute la théorie des asymptotes rectilignes; la courbe représentée par l'équation (1), où x et y désignent alors des coordonnées rectilignes, a pour asymptote réelle ou imaginaire la droite représentée par l'équation

(16) $$y = \alpha x + \alpha'.$$

La différence ε' qui existe entre les coordonnées de la courbe et de l'asymptote est généralement un *infiniment petit du premier ordre*, en considérant $\frac{1}{x}$ lui-même comme un infiniment petit du premier ordre.

La courbe représentée par l'équation (1) admet aussi

pour asymptote l'hyperbole que représente l'équation

$$(17) \qquad y = \alpha x + \alpha' + \frac{\alpha''}{x};$$

mais dans ce cas la différence $\frac{\varepsilon''}{x}$ des ordonnées des deux courbes est un infiniment petit du second ordre au moins.

La courbe (17) pourrait être appelée *asymptote du deuxième ordre* de la courbe proposée. Et, comme on peut pousser aussi loin que l'on veut le développement de y en série ordonnée suivant les puissances décroissantes de x, on pourra former une infinité de courbes des degrés respectifs 3, 4, etc., et qui auront, avec la courbe proposée, un asymptotisme de plus en plus intime.

On voit aisément, sans qu'il soit nécessaire d'insister sur ce sujet, comment il faudrait modifier la méthode, si l'équation

$$f(\alpha) = 0$$

avait des racines égales, contrairement à l'hypothèse que nous avons faite.

Formation de l'équation finale résultant de l'élimination d'une inconnue entre deux équations à deux inconnues. Nouvelle démonstration du théorème de Bezout. Somme des racines de l'équation finale.

La théorie qui vient d'être exposée permet de former autant de termes que l'on veut de l'équation finale résultant de l'élimination d'une inconnue entre deux équations. Soient les deux équations générales

$$(1) \qquad \begin{cases} M(x, y) = 0, \\ N(x, y) = 0, \end{cases}$$

des degrés m et n respectivement; en réunissant les termes de même degré, on pourra les écrire de la manière sui-

vante :

$$(2)\quad \begin{cases} x^m f\left(\frac{y}{x}\right) + x^{m-1} f_1\left(\frac{y}{x}\right) + x^{m-2} f_2\left(\frac{y}{x}\right) + \ldots = 0, \\ x^n \mathrm{F}\left(\frac{y}{x}\right) + x^{n-1} \mathrm{F}_1\left(\frac{y}{x}\right) + x^{n-2} \mathrm{F}_2\left(\frac{y}{x}\right) + \ldots = 0. \end{cases}$$

f, f_1, f_2, etc., sont des polynômes respectivement des degrés m, $m-1$, $m-2$, etc.; F, F_1, F_2, etc., des polynômes des degrés n, $n-1$, $n-2$, etc.

Soient $y_1, y_2, \ldots, y_n$ les valeurs de y tirées de la première des équations (1), portons-les dans le premier membre de la seconde, et désignons par V le produit des résultats ainsi obtenus, de manière que l'on ait

$$(3)\qquad \mathrm{V} = \mathrm{N}(x, y_1)\,\mathrm{N}(x, y_2)\ldots \mathrm{N}(x, y_m);$$

l'équation finale résultant de l'élimination de y sera

$$\mathrm{V} = 0.$$

On calculera aisément la fonction V, en développant en série suivant les puissances décroissantes de x, chacun de ses facteurs, dont l'expression générale est $\mathrm{N}(x, y)$. Je dis même que, si l'on ne veut connaître que le premier terme de V, il suffit de borner les séries dont nous parlons à leur premier terme; que, si l'on ne veut que les deux premiers termes de V, il suffit de connaître les deux premiers termes des séries, et ainsi de suite.

Supposons, par exemple, qu'on ne veuille connaître que le premier terme de V; on a, en faisant comme précédemment $u = \frac{y}{x}$,

$$\mathrm{N}(x, y) = x^n \mathrm{F}(u) + x^{n-1} \mathrm{F}_1(u) + \ldots.$$

Posons aussi, comme plus haut,

$$u = \alpha + \varepsilon,$$

ε étant une quantité qui s'annule avec $\frac{1}{x}$, et α une racine quelconque de l'équation

$$f(\alpha) = 0;$$

on aura

$$\frac{N(x, y)}{x^n} = F(\alpha + \varepsilon) + \frac{1}{x} F_1(\alpha + \varepsilon) + \ldots,$$

et pour $x = \infty$,

$$\lim \frac{N(x, y)}{x^n} = F(\alpha),$$

ou

$$N(x, y) = x^n F(\alpha) + x^n E, \tag{4}$$

E désignant une quantité qui s'annule avec $\frac{1}{x}$. D'après cela, en représentant par

$$\alpha_1, \alpha_2, \ldots, \alpha_m$$

les m valeurs de α, on aura

$$N(x, y_1) = x^n F(\alpha_1) + x^n E_1,$$
$$N(x, y_2) = x^n F(\alpha_2) + x^n E_2,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$N(x, y_m) = x^n F(\alpha_m) + x^n E_m,$$

$E_1, E_2, \ldots, E_m$ désignant des quantités qui s'évanouissent avec $\frac{1}{x}$. Multipliant ces équations et ayant égard à l'équation (3), on aura

$$V = x^{mn} F(\alpha_1) F(\alpha_2) \ldots F(\alpha_m) + x^{mn} H, \tag{5}$$

H désignant une quantité qui s'annule avec $\frac{1}{x}$.

Le premier terme de V est donc

$$x^{mn} F(\alpha_1) F(\alpha_2) \ldots F(\alpha_m);$$

on pourra l'exprimer en fonction rationnelle des coefficients de F et f, puisque $F(\alpha_1)F(\alpha_2)\ldots F(\alpha_m)$ est une fonction symétrique et entière des racines de l'équation

$$f(\alpha)=0.$$

Il suit de là que l'équation finale résultant de l'élimination de y entre les équations (1) et (2) est d'un degré égal au produit des degrés de ces équations.

Remarque. — Si les coefficients des équations (1) ont des valeurs déterminées, et que ces équations contiennent la plus haute puissance de y, l'équation finale résultant de l'élimination de y sera toujours $V=0$, et l'on voit que le degré de cette équation finale sera encore égal au produit des degrés des équations proposées, à moins que les équations

$$f(\alpha)=0, \quad F(\alpha)=0$$

n'aient une ou plusieurs racines communes, auquel cas ce degré s'abaisse nécessairement.

Pour avoir les deux premiers termes de l'équation finale $V=0$, il faut connaître les deux premiers termes du développement de $N(x, y)$ en série. Pour cela, dans l'équation

$$N(x, y)=x^n F(u)+x^{n-1}F_1(u)+\ldots,$$

nous poserons

$$u=\alpha+\frac{\alpha'}{x}+\frac{\varepsilon'}{x},$$

ε' étant toujours une quantité qui s'évanouit avec $\frac{1}{x}$, α une racine de

$$f(\alpha)=0,$$

et α' une quantité que nous avons calculée, et qui est déterminée par l'équation

$$\alpha' f'(\alpha)+f_1(\alpha)=0;$$

on aura alors

$$N(x, y) = x^n F(\alpha) + x^{n-1}[\alpha' F'(\alpha) + F_1(\alpha)] + x^{n-1} E,$$

E désignant une quantité qui s'annule avec $\frac{1}{x}$. Cette formule donne le développement de $N(x, y)$, borné aux deux premiers termes; en y remplaçant α par chacune de ses m valeurs, on aura

$$N(x, y_1) = x^n F(\alpha_1) + x^{n-1}[\alpha'_1 F'(\alpha_1) + F_1(\alpha_1)] + x^{n-1} E_1,$$
$$N(x, y_2) = x^n F(\alpha_2) + x^{n-1}[\alpha'_2 F'(\alpha_2) + F_1(\alpha_2)] + x^{n-1} E_2,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$N(x, y_m) = x^n F(\alpha_m) + x^{n-1}[\alpha'_m F'(\alpha_m) + F_1(\alpha_m)] + x^{n-1} E_m.$$

Dans ces équations, E_1, E_2, etc., sont des quantités qui s'évanouissent avec $\frac{1}{x}$, et α'_1, α'_2, etc., les valeurs de α', qui correspondent aux valeurs α_1, α_2, etc., de α. Multipliant toutes ces équations, ayant égard à l'équation (3), et désignant simplement par $x^{mn-1} H$ l'ensemble des termes dont le quotient par x^{mn-1} s'annule avec $\frac{1}{x}$, on aura

$$V = x^{mn} F(\alpha_1) F(\alpha_2) \ldots F(\alpha_m)$$
$$+ x^{mn-1} F(\alpha_1) F(\alpha_2) \ldots F(\alpha_m) \sum \frac{\alpha' F'(\alpha) + F_1(\alpha)}{F(\alpha)} + x^{mn-1} H.$$

Dans cette dernière formule, la quantité H, qui est infiniment petite avec $\frac{1}{x}$, contient un nombre limité de termes, et l'on voit que le second terme de V aura pour coefficient

$$F(\alpha_1) F(\alpha_2) \ldots F(\alpha_m) \sum \frac{\alpha' F'(\alpha) + F_1(\alpha)}{F(\alpha)},$$

le signe $\sum$ s'étendant à toutes les racines α de l'équation

$$f(\alpha) = 0.$$

D'après cela, si l'on désigne par $\sum x$ la somme des racines de l'équation finale en x, on aura

$$\sum x = -\sum \frac{\alpha' F'(\alpha) + F_1(\alpha)}{F(\alpha)},$$

ou en mettant, au lieu de α', sa valeur $-\frac{f_1(\alpha)}{f'(\alpha)}$,

$$\sum x = \sum \frac{f_1(\alpha)\, F'(\alpha)}{f'(\alpha)\, F(\alpha)} - \sum \frac{F_1(\alpha)}{F(\alpha)}.$$

On pourrait calculer ainsi autant de termes que l'on voudrait de l'équation finale $V = 0$; par suite, cette équation tout entière : seulement les calculs deviennent de plus en plus compliqués, et nous nous bornerons à ce qui précède.

Nouvelle démonstration d'une formule d'analyse.

Au lieu de porter dans l'équation $N = 0$ les valeurs de y tirées de $M = 0$, afin d'avoir l'équation finale $V = 0$, on aurait pu faire l'inverse, porter dans l'équation $M = 0$ les valeurs de y tirées de $N = 0$; mais alors on aurait eu une autre expression de la somme $\sum x$ des racines de l'équation finale, que l'on peut écrire sans faire de nouveaux calculs. On aura, en effet, évidemment

$$\sum x = \sum \frac{F_1(6) f'(6)}{F'(6) f(6)} - \sum \frac{f_1(6)}{f(6)},$$

les sommes du second membre s'étendant à toutes les racines 6 de l'équation

$$F(6) = 0;$$

en égalant entre elles ces deux valeurs de $\sum x$, on aura

$$\sum \frac{f_1(\alpha)\, F'(\alpha)}{f'(\alpha)\, F(\alpha)} - \sum \frac{F_1(\alpha)}{F(\alpha)} = \sum \frac{F_1(6) f'(6)}{F'(6) f(6)} - \sum \frac{f_1(6)}{f(6)},$$

les sommes du premier membre étant relatives aux racines α de $f(\alpha) = 0$, celles du second aux racines 6 de $F(6) = 0$. Dans cette formule, qui exprime un théorème d'analyse, f et F désignent des polynômes quelconques, mais n'ayant ni racines égales, ni racines communes; f_1 et F_1 désignent aussi des polynômes quelconques, mais de degrés respectivement moindres que f et F.

Supposons que le polynôme F soit égal à f_1, et que F_1 soit identiquement nul; l'équation précédente se réduit à

$$\sum \frac{F'(\alpha)}{f'(\alpha)} = -\sum \frac{F(6)}{f(6)},$$

ou même à

$$\sum \frac{F'(\alpha)}{f'(\alpha)} = 0,$$

puisque chaque terme du second membre est nul, le signe $\sum$ étant relatif aux racines de $F(6) = 0$. Dans l'équation précédente, le signe $\sum$ s'étend aux racines α de $f(\alpha) = 0$, et F' désigne la dérivée d'un polynôme quelconque F de degré inférieur à f; par conséquent, F' est un polynôme quelconque de degré inférieur à f'. La formule précédente est, comme nous l'avons vu, celle dont M. Liouville a déduit la décomposition des fractions rationnelles en fractions simples.

Démonstration d'un théorème de géométrie.

M. Liouville a appliqué les recherches précédentes à la démonstration d'un théorème curieux de géométrie, que nous allons présenter ici :

Si l'on mène à une courbe algébrique la série des tangentes parallèles à une direction donnée, le centre des

moyennes distances des points de contact sera indépendant de cette direction.

Soit

$$M(x, y) = 0$$

l'équation d'une courbe algébrique; les coordonnées réelles ou imaginaires des points de contact de cette courbe, avec les tangentes parallèles à la droite $y = ax$, seront les solutions communes aux deux équations

$$(1) \qquad M = 0, \quad \frac{dM}{dx} + a\frac{dM}{dy} = 0.$$

Si l'on pose $\frac{y}{x} = u$ et qu'on représente la courbe par l'équation $\varphi(x, u) = 0$, les coordonnées x et u seront les solutions communes aux deux équations

$$\varphi(x, u) = 0, \quad \frac{d\varphi}{dx} + \frac{a-u}{x}\frac{d\varphi}{du} = 0.$$

Soit donc, en conservant les notations employées précédemment,

$$\varphi(x, u) = x^m f(u) + x^{m-1} f_1(u) + \ldots,$$

f, f_1, etc., désignant des polynômes des degrés m, $m-1$, etc.; on aura

$$\frac{d\varphi}{dx} = mx^{m-1} f(u) + (m-1)x^{m-2} f_1(u) + \ldots,$$

$$\frac{d\varphi}{du} = x^m f'(u) + x^{m-1} f_1'(u) + \ldots,$$

et, par suite,

$$\frac{d\varphi}{dx} + \frac{a-u}{x}\frac{d\varphi}{du} = x^{m-1} F(u) + x^{m-2} F_1(u) + \ldots,$$

en faisant, pour abréger,

$$(2) \qquad \begin{cases} F(u) = mf(u) + (a-u) f'(u), \\ F_1(u) = (m-1) f_1(u) + (a-u) f_1'(u), \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

$F(u)$, $F_1(u)$, etc., sont des polynômes des degrés $m-1$, $m-2$, etc.; car dans $F(u)$ par exemple, les deux termes du degré le plus élevé, qui proviennent de $mf(u)$ et $(a-u)f'(u)$, se détruisent évidemment; et la même chose a lieu pour $F_1(u)$, etc.

L'équation finale résultant de l'élimination de y entre les équations (1) est donc la même que celle qui résulte de l'élimination de u entre

$$x^m f(u) + x^{m-1} f_1(u) + \ldots\ldots = 0,$$
$$x^{m-1} F(u) + x^{m-2} F_1(u) + \ldots = 0.$$

Si donc on désigne, comme précédemment, par $\sum x$ la somme des racines de l'équation finale, on aura

$$\sum x = -\sum \frac{\alpha' F'(\alpha) + F_1(\alpha)}{F(\alpha)},$$

le signe $\sum$ s'étendant dans le second membre aux racines de l'équation

$$f(\alpha) = 0,$$

et α' étant une quantité déterminée par l'équation

$$\alpha' f'(\alpha) + f_1(\alpha) = 0.$$

Pour avoir l'expression de $\sum x$ en fonction des quantités données f, f_1, etc., différentions la première des équations (2); on aura

$$F'(u) = (m-1) f'(u) + (a-u) f''(u). \tag{3}$$

Les équations (2) et (3) donnent ensuite

$$\alpha' F'(\alpha) + F_1(\alpha) = (m-1)[\alpha' f'(\alpha) + f_1(\alpha)] + (a-\alpha)[\alpha' f''(\alpha) + f_1'(\alpha)],$$

et, comme $\alpha' f'(\alpha) + f_1(\alpha)$ est nul,

$$\alpha' F'(\alpha) + F_1(\alpha) = (a-\alpha)[\alpha' f''(\alpha) + f_1'(\alpha)]; \tag{4}$$

on aura aussi, en faisant $u = \alpha$ dans la première des équations (2), et remarquant que $f(\alpha)$ est nul,

$$F(\alpha) = (a - \alpha) f'(\alpha). \tag{5}$$

Des équations (4) et (5) on tire

$$\frac{\alpha' F'(\alpha) + F_1(\alpha)}{F(\alpha)} = \frac{\alpha' f''(\alpha) + f_1'(\alpha)}{f'(\alpha)};$$

par suite, la valeur de $\sum x$ est

$$\sum x = -\sum \frac{\alpha' f''(\alpha) + f_1'(\alpha)}{f'(\alpha)}.$$

On voit qu'elle ne contient pas a. La somme des distances à l'axe des y des points de contact de notre courbe avec les tangentes parallèles à la direction donnée est donc indépendante de cette direction; ce qui démontre le théorème énoncé, car l'axe des y est une droite quelconque située dans le plan.

Remarque. — La démonstration précédente semble en défaut lorsque l'équation $f(\alpha) = 0$ a des racines égales; pour montrer que les conclusions sont cependant exactes dans ce cas, on peut employer un raisonnement dont nous avons déjà plusieurs fois fait usage. Il suffira de modifier insensiblement les coefficients de f, de manière que $f(\alpha) = 0$ n'ait plus de racines égales : on aura une courbe infiniment peu différente de la proposée, et pour laquelle le théorème aura lieu; d'où l'on peut conclure qu'il a lieu, à la limite, pour la courbe proposée elle-même.

Corollaire. — Désignons toujours par $\sum x$ la somme des abscisses des points de contact d'une courbe algébrique avec les tangentes qui font l'angle ω avec la direction des x positives, et faisons varier ω de sa dif-

férentielle $d\omega$; comme $\sum x$ ne dépend pas de cet angle, on aura

$$\sum dx = 0.$$

Mais, en désignant par ds l'arc infiniment petit qui a pour projection dx, on a $dx = ds \cos\omega$; par suite

$$\sum ds \cos\omega = 0, \quad \text{ou} \quad \sum \frac{ds}{d\omega} = 0,$$

puisque $\cos\omega$ et $d\omega$ sont constants. $\frac{ds}{d\omega}$ est la valeur du rayon de courbure ρ, on aura donc

$$\sum \rho = 0;$$

on aura aussi

$$\sum \frac{d\rho}{d\omega} = 0, \quad \text{ou} \quad \sum \rho' = 0,$$

ρ' désignant le rayon de courbure de la développée, et ainsi de suite.

En outre, si ξ et υ représentent les coordonnées du centre de courbure correspondant au point (x, y), on a

$$x = \xi - \rho \sin\omega, \quad y = \upsilon + \rho \cos\omega;$$

donc, en ayant égard aux formules précédentes,

$$\sum x = \sum \xi, \quad \sum y = \sum \upsilon;$$

c'est-à-dire que le centre des moyennes distances des points de contact d'une courbe algébrique avec la série des tangentes parallèles à une même direction, est le même que le centre des moyennes distances des centres de courbure correspondants.

DIXIÈME LEÇON.

Développement en séries ordonnées suivant les puissances décroissantes de la variable de deux ou plusieurs fonctions algébriques définies par deux ou plusieurs équations. — Formation de l'équation finale résultant de l'élimination de deux, trois, etc., inconnues entre trois, quatre, etc., équations. Nouvelle démonstration du théorème de Bezout. Somme des racines de l'équation finale. — Démonstration d'une formule de M. Jacobi. — Extension du théorème de géométrie démontré dans la leçon précédente.

L'analyse que nous avons développée dans la dernière leçon peut être aisément généralisée, et étendue à l'élimination de deux, trois, etc., inconnues entre trois, quatre, etc., équations. C'est ce que nous allons établir, en adoptant pour l'exposition le même ordre que dans la leçon précédente.

Développement en séries ordonnées suivant les puissances décroissantes de la variable, de deux ou plusieurs fonctions algébriques définies par deux ou plusieurs équations.

Soient

$$M(x, y, z) = 0, \quad N(x, y, z) = 0 \tag{1}$$

deux équations générales des degrés m et n respectivement entre les trois variables x, y, z; la première x étant considérée comme indépendante, les deux autres y et z en seront des fonctions. En réunissant les termes de même degré, les équations (1) pourront s'écrire de la manière suivante :

$$\left\{\begin{aligned} &x^m f\left(\frac{y}{x}, \frac{z}{x}\right) + x^{m-1} f_1\left(\frac{y}{x}, \frac{z}{x}\right) + \ldots = 0, \\ &x^n F\left(\frac{y}{x}, \frac{z}{x}\right) + x^{n-1} F_1\left(\frac{y}{x}, \frac{z}{x}\right) + \ldots = 0, \end{aligned}\right. \tag{2}$$

ou, en posant $\frac{y}{x} = u$, $\frac{z}{x} = v$,

$$(3)\qquad \begin{cases} x^m f(u, v) + x^{m-1} f_1(u, v) + \ldots = 0, \\ x^n \mathrm{F}(u, v) + x^{n-1} \mathrm{F}_1(u, v) + \ldots = 0. \end{cases}$$

f et F sont des polynômes des degrés m et n respectivement, entre les variables u et v; f_1 et F_1 sont respectivement des degrés $m-1$ et $n-1$, et ainsi des autres.

En vertu des résultats obtenus dans la leçon précédente, le nombre des solutions communes (u, v) aux équations (3) est mn, ainsi que le nombre des solutions communes $(\alpha, 6)$ aux équations

$$(4)\qquad f(\alpha, 6) = 0, \quad \mathrm{F}(\alpha, 6) = 0;$$

et les mn systèmes de solutions communes des équations (3) se réduiront, pour $x = \infty$, aux mn systèmes de solutions communes des équations (4). On pourra donc poser généralement

$$(5)\qquad u = \alpha + \varepsilon, \quad v = 6 + \eta,$$

ε et η désignant des quantités qui s'annulent avec $\frac{1}{x}$. Ces quantités sont d'ailleurs les restes des séries dans lesquelles u et v se développent quand on borne ces séries à leur premier terme. Pour calculer les limites des produits εx, ηx, nous suivrons la même marche que dans la leçon précédente. En portant dans les équations (3) les valeurs de u et v, tirées de (5), et ayant égard aux équations (4), on a

$$x^m\left(\varepsilon \frac{df}{d\alpha} + \eta \frac{df}{d6} + \ldots\right) + x^{m-1}[f_1(\alpha, 6) + \ldots] + \ldots = 0,$$

$$x^n\left(\varepsilon \frac{d\mathrm{F}}{d\alpha} + \eta \frac{d\mathrm{F}}{d6} + \ldots\right) + x^{n-1}[\mathrm{F}_1(\alpha, 6) + \ldots] + \ldots = 0.$$

En divisant ces équations respectivement par x^{m-1} et

x^{n-1}, faisant ensuite $x = \infty$, et posant

$$\alpha' = \lim \varepsilon x, \quad 6' = \lim \eta x;$$

on obtient

$$(6)\quad \begin{cases} \alpha' \dfrac{df}{d\alpha} + 6' \dfrac{df}{d6} + f_1 = 0, \\ \alpha' \dfrac{dF}{d\alpha} + 6' \dfrac{dF}{d6} + F_1 = 0; \end{cases}$$

d'où l'on tire les valeurs suivantes de α' et $6'$:

$$(7)\quad \begin{cases} \alpha' = \dfrac{F_1 \dfrac{df}{d6} - f_1 \dfrac{dF}{d6}}{\dfrac{df}{d\alpha}\dfrac{dF}{d6} - \dfrac{df}{d6}\dfrac{dF}{d\alpha}}, \\ 6' = \dfrac{f_1 \dfrac{dF}{d\alpha} - F_1 \dfrac{df}{d\alpha}}{\dfrac{df}{d\alpha}\dfrac{dF}{d6} - \dfrac{df}{d6}\dfrac{dF}{d\alpha}}. \end{cases}$$

En désignant par ε' et η' de nouvelles quantités infiniment petites avec $\frac{1}{x}$, on pourra poser

$$\varepsilon x = \alpha' + \varepsilon', \quad \eta x = 6' + \eta',$$

et, par suite,

$$u = \alpha + \frac{\alpha'}{x} + \frac{\varepsilon'}{x}, \quad v = 6 + \frac{6'}{x} + \frac{\eta'}{x};$$

on a ainsi les deux premiers termes des séries dans lesquelles u et v, ou y et z peuvent se développer, et l'on voit aisément qu'on pourra, de la même manière, obtenir les termes suivants.

La même méthode s'appliquera, sans modification, au cas de $\mu - 1$ équations entre μ variables, pourvu qu'on écarte, comme nous l'avons fait jusqu'ici, en raisonnant sur des équations générales, quelques cas particuliers qui peuvent se présenter.

Formation de l'équation finale résultant de l'élimination de deux, trois, etc., inconnues entre trois, quatre, etc., équations. Nouvelle démonstration du théorème de Bezout. Somme des racines de l'équation finale.

On peut, par l'analyse précédente, former autant de termes que l'on veut, de l'équation finale résultant de l'élimination de deux, trois, etc., inconnues, entre trois, quatre, etc., équations.

Soient, par exemple, les trois équations générales

$$(1)\quad M(x, y, z) = 0, \quad N(x, y, z) = 0, \quad P(x, y, z) = 0,$$

des degrés m, n, p respectivement, entre trois inconnues x, y, z; en réunissant les termes de même degré, ces équations seront :

$$x^m f\left(\frac{y}{x}, \frac{z}{x}\right) + x^{m-1} f_1\left(\frac{y}{x}, \frac{z}{x}\right) + \ldots = 0,$$

$$x^n \mathrm{F}\left(\frac{y}{x}, \frac{z}{x}\right) + x^{n-1} \mathrm{F}_1\left(\frac{y}{x}, \frac{z}{x}\right) + \ldots = 0,$$

$$x^p \varphi\left(\frac{y}{x}, \frac{z}{x}\right) + x^{p-1} \varphi_1\left(\frac{y}{x}, \frac{z}{x}\right) + \ldots = 0.$$

f, F et φ sont des polynômes des degrés m, n, p respectivement, par rapport aux deux variables qu'ils renferment; f_1, F_1, φ_1 sont respectivement des degrés $m-1$, $n-1$, $p-1$, et ainsi de suite.

Désignons par

$$(y_1, z_1), \quad (y_2, z_2), \ldots, \quad (y_{mn}, z_{mn})$$

les mn systèmes de solutions communes aux deux premières des équations (1), et posons

$$V = P(x, y_1, z_1)\,P(x, y_2, z_2)\ldots\,P(x, y_{mn}\ z_{mn});$$

l'équation finale résultant de l'élimination de y et z entre

les équations (1) sera

$$V = 0,$$

et c'est cette équation qu'il s'agit de calculer. On y parviendra en développant en série chacun des facteurs $P(x, y, z)$ de V, et il suffira de connaître autant de termes du développement de P qu'on en veut avoir dans V. Nous nous bornerons ici, comme nous l'avons fait dans la leçon précédente, à calculer les deux premiers termes de V, ce qui suffit pour connaître le degré et la somme des racines de l'équation finale.

On a, en faisant, comme précédemment, $\frac{y}{x} = u$, $\frac{z}{x} = v$,

$$P(x, y, z) = x^p \varphi(u, v) + x^{p-1} \varphi_1(u, v) + \ldots,$$

et, si l'on pose

$$u = \alpha + \varepsilon, \quad v = 6 + \eta,$$

il vient

$$P(x, y, z) = x^p \varphi(\alpha, 6) + x^p E,$$

E s'annulant avec $\frac{1}{x}$, ainsi que ε et η. En mettant dans l'équation précédente, à la place de x et y, leurs mn valeurs, il vient

$$P(x, y_1, z_1) = x^p \varphi(\alpha_1, 6_1) + x^p E_1,$$
$$P(x, y_2, z_2) = x^p \varphi(\alpha_2, 6_2) + x^p E_2,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$P(x, y_{mn}, z_{mn}) = x^p \varphi(\alpha_{mn}, 6_{mn}) + x^p E_{mn},$$

$E_1, E_2, \ldots, E_{mn}$ étant des quantités infiniment petites avec $\frac{1}{x}$. Enfin, en multiplant toutes ces équations, on a la valeur suivante de V,

$$V = x^{mnp} \varphi(\alpha_1, 6_1) \varphi(\alpha_2, 6_2) \ldots \varphi(\alpha_{mn}, 6_{mn}) + x^{mnp} H,$$

où H désigne une quantité qui s'annule avec $\frac{1}{x}$. Le premier

terme de V sera donc

$$x^{mnp}\varphi(\alpha_1, 6_1)\ldots\varphi(\alpha_{mn}, 6_{mn}).$$

Il suit de là que le degré de l'équation finale résultant de l'élimination de y et z entre les trois équations (1) est égal au produit des degrés de ces équations, ce qui fournit une nouvelle démonstration du théorème de Bezout.

Si l'on veut obtenir les deux premiers termes de l'équation finale $V = 0$, il est nécessaire de calculer les deux premiers termes du développement de $P(x, y, z)$ en série ordonnée suivant les puissances décroissantes de x. Pour cela, dans l'équation

$$P(x, y, z) = x^p\varphi(u, v) + x^{p-1}\varphi_1(u, v) + \ldots$$

nous poserons

$$u = \alpha + \frac{\alpha'}{x} + \frac{\varepsilon'}{x},$$

$$v = 6 + \frac{6'}{x} + \frac{\eta'}{x},$$

ε' et η' désignant toujours des quantités qui s'évanouissent avec $\frac{1}{x}$, α' et $6'$ des quantités déterminées par les équations

$$\alpha'\frac{df}{d\alpha} + 6'\frac{df}{d6} + f_1 = 0,$$

$$\alpha'\frac{dF}{d\alpha} + 6'\frac{dF}{d6} + F_1 = 0.$$

La valeur de $P(x, y, z)$ pourra alors s'écrire de la manière suivante :

$$P(x, y, z) = x^p\varphi(\alpha, 6)$$

$$+ x^{p-1}\left[\alpha'\frac{d\varphi}{d\alpha} + 6'\frac{d\varphi}{d6} + \varphi_1(\alpha, 6)\right] + x^{p-1}E,$$

en désignant par E une quantité qui s'annule avec $\frac{1}{x}$; on

aura donc

$$P(x, y_1, z_1) = x^p \varphi(\alpha_1, 6_1)$$
$$+ x^{p-1}\left[\alpha'_1 \frac{d\varphi}{d\alpha_1} + 6'_1 \frac{d\varphi}{d6_1} + \varphi_1(\alpha_1, 6_1)\right] + x^{p-1} E_1,$$

. . . .

. . . .

$$P(x, y_{mn}, z_{mn}) = x^p \varphi(\alpha_{mn}, 6_{mn})$$
$$+ x^{p-1}\left[\alpha'_{mn} \frac{d\varphi}{d\alpha_{mn}} + 6'_{mn} \frac{d\varphi}{d6_{mn}} + \varphi_1(\alpha_{mn}, 6_{mn})\right] + x^{p-1} E_{mn}.$$

Dans ces équations nous avons mis, pour abréger, $\frac{d\varphi}{d\alpha_1}$, etc., à la place de $\frac{d\varphi(\alpha_1, 6_1)}{d\alpha_1}$, etc.; α'_1, α'_2, etc., désignent les valeurs de α' qui correspondent aux valeurs α_1, α_2, etc., de α; enfin, E_1, E_2, etc., sont des quantités infiniment petites avec $\frac{1}{x}$. En multipliant toutes ces équations, on aura la valeur suivante de V :

$$V = x^{mnp} \varphi(\alpha_1, 6_1) \varphi(\alpha_2, 6_2) \ldots \varphi(\alpha_{mn}, 6_{mn})$$
$$+ x^{mnp-1} \varphi(\alpha_1, 6_1) \ldots \varphi(\alpha_{mn}, 6_{mn}) \sum \frac{\alpha' \frac{d\varphi}{d\alpha} + 6' \frac{d\varphi}{d6} + \varphi_1(\alpha, 6)}{\varphi(\alpha, 6)}$$
$$+ x^{mnp-1} H,$$

où H désigne une quantité qui s'annule avec $\frac{1}{x}$, et où le signe $\sum$ s'étend à toutes les solutions communes $(\alpha, 6)$, des deux équations

$$f(\alpha, 6) = 0, \quad F(\alpha, 6) = 0.$$

Le second terme de V est donc

$$x^{mnp-1} \varphi(\alpha_1, 6_1) \ldots \varphi(\alpha_{mn}, 6_{mn}) \sum \frac{\alpha' \frac{d\varphi}{d\alpha} + 6' \frac{d\varphi}{d6} + \varphi_1}{\varphi} :$$

et si l'on désigne par $\sum x$ la somme des racines de l'équation finale $V = 0$, on aura

$$\sum x = -\sum \frac{\alpha' \frac{d\varphi}{d\alpha} + 6' \frac{d\varphi}{d6} + \varphi_1}{\varphi}.$$

En remplaçant, dans cette formule, α' et $6'$ par leurs valeurs écrites plus haut, et faisant, pour abréger,

$$A_1(\alpha, 6) = \frac{dF}{d\alpha}\frac{d\varphi}{d6} - \frac{d\varphi}{d\alpha}\frac{dF}{d6},$$

$$B(\alpha, 6) = \frac{d\varphi}{d\alpha}\frac{df}{d6} - \frac{df}{d\alpha}\frac{d\varphi}{d6},$$

$$C(\alpha, 6) = \frac{df}{d\alpha}\frac{dF}{d6} - \frac{dF}{d\alpha}\frac{df}{d6},$$

on aura cette expression

$$\sum x = -\sum \frac{\varphi_1(\alpha, 6)}{\varphi(\alpha, 6)} - \sum \frac{f_1(\alpha, 6)\, A(\alpha, 6) + F_1(\alpha, 6)\, B(\alpha, 6)}{\varphi(\alpha, 6)\, C(\alpha, 6)},$$

où les sommes du second membre sont relatives à tous les couples de solutions communes aux deux équations

$$f(\alpha, 6) = 0, \quad F(\alpha, 6) = 0.$$

Le calcul des deux premiers termes de l'équation finale, qui résulterait de l'élimination de $\mu - 1$ inconnues entre μ équations, n'offrira pas plus de difficulté, quel que soit μ, que dans les deux cas particuliers que nous avons développés; la marche à suivre est toujours la même, et l'on peut considérer comme générale la nouvelle démonstration que nous avons donnée du théorème de Bezout pour le cas de deux ou trois équations.

Démonstration d'une formule de M. Jacobi.

Pour obtenir l'équation finale $V = 0$, nous avons porté

dans la troisième des équations données les valeurs de y et z, tirées des deux premières; mais on aurait pu opérer de deux autres manières différentes: on aurait pu, par exemple, porter dans la première les valeurs de y et z, tirées des deux dernières, et l'on aurait obtenu une expression différente de $\sum x$, qui se déduirait évidemment de celle déjà trouvée, en changeant l'une en l'autre f et φ, f_1 et φ_1, etc. On aura donc

$$\sum x = -\sum \frac{f_1(\gamma, \delta)}{f(\gamma, \delta)} - \sum \frac{F_1(\gamma, \delta)\, B(\gamma, \delta) + \varphi_1(\gamma, \delta)\, C(\gamma, \delta)}{f(\gamma, \delta)\, A(\gamma, \delta)};$$

mais ici les sommes qui figurent dans le second membre sont relatives aux solutions communes des équations

$$F(\gamma, \delta) = 0, \quad \varphi(\gamma, \delta) = 0.$$

Égalons les deux valeurs trouvées pour $\sum x$, et supposons que les polynômes F_1 et f_1 soient identiquement nuls; on aura

$$\sum \frac{\varphi_1(\alpha, 6)}{\varphi(\alpha, 6)} = \sum \frac{\varphi_1(\gamma, \delta)\, C(\gamma, \delta)}{f(\gamma, \delta)\, A(\gamma, \delta)},$$

en se rappelant que le signe $\sum$ s'étend dans le premier membre aux solutions communes de $f(\alpha, 6) = 0$, $F(\alpha, 6) = 0$, et dans le second membre aux solutions communes de $F(\gamma, \delta) = 0$, $\varphi(\gamma, \delta) = 0$. On peut, dans cette formule, considérer les polynômes f, F et φ comme absolument arbitraires; et, quant au polynôme φ_1, il n'est assujetti, par notre analyse, qu'à la seule condition d'être de degré inférieur à φ. Supposons

$$\varphi(\alpha, 6) = C(\alpha, 6);$$

la somme du second membre de l'équation précédente sera alors relative aux solutions communes des deux équations

$$F(\gamma, \delta) = 0, \quad C(\gamma, \delta) = 0,$$

et, par conséquent, chacun de ses termes sera identiquement nul. On aura donc

$$\sum \frac{\varphi_1(\alpha, 6)}{C(\alpha, 6)} = 0$$

ou

$$\sum \frac{\varphi_1(\alpha, 6)}{\frac{df}{d\alpha}\frac{dF}{d\beta} - \frac{dF}{d\alpha}\frac{df}{d\beta}} = 0,$$

le signe $\sum$ s'étendant aux solutions communes des deux équations

$$f(\alpha, 6) = 0, \quad F(\alpha, 6) = 0.$$

Cette formule curieuse, où φ_1 désigne un polynôme quelconque de degré inférieur à celui de $\frac{df}{d\alpha}\frac{dF}{d\beta} - \frac{dF}{d\alpha}\frac{df}{d\beta}$, est l'extension de celle que nous avons démontrée dans la cinquième leçon, et à laquelle nous avons été de nouveau conduit dans la leçon précédente. Elle a été démontrée pour la première fois par M. Jacobi, et M. Liouville l'a trouvée, ainsi que nous venons de le faire voir, comme une conséquence naturelle de ses recherches sur l'élimination.

Extension du théorème de géométrie démontré dans la leçon précédente.

M. Liouville a donné dans son Mémoire la démonstration du théorème suivant, qui est l'extension de celui que nous avons établi dans la dernière leçon :

THÉORÈME. — *Si l'on mène à une surface algébrique la série des plans tangents parallèles à deux directions fixes, le centre des moyennes distances des points de contact sera indépendant de ces deux directions.*

Si

$$M(x, y, z) = 0$$

est l'équation d'une surface algébrique, les coordonnées des points de contact de cette surface avec les plans tangents parallèles au plan qui a pour équation

$$z = ax + by,$$

seront données par les trois équations

$$M = 0, \quad \frac{dM}{dx} + a\frac{dM}{dz} = 0, \quad \frac{dM}{dy} + b\frac{dM}{dz} = 0.$$

Il suffit, pour établir le théorème qui vient d'être énoncé, de calculer la somme des racines de l'équation finale résultant de l'élimination de deux inconnues entre les trois équations précédentes. En suivant la marche que nous avons tracée, on trouvera que cette somme est indépendante de a et de b. Ce calcul ne présentant aucune difficulté, nous nous dispenserons de le présenter ici, et nous renverrons, pour plus de détails, au Mémoire de M. Liouville. On y trouvera, du reste, un grand nombre de conséquences curieuses que nous ne pourrions développer sans sortir des limites que nous nous sommes imposées.

ONZIÈME LEÇON.

Théorème sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme. — Des fonctions semblables. — Propriété des fonctions semblables des racines d'une équation. — Examen des cas particuliers qui font exception. — Méthode pour calculer une fonction des racines d'une équation, quand on connaît une autre fonction quelconque des racines.

Parmi les travaux publiés depuis un siècle sur la théorie algébrique des équations, l'un des plus importants est, sans contredit, le célèbre Mémoire de Lagrange, que nous avons déjà eu l'occasion de citer, et qui fait partie des *Mémoires de l'Académie de Berlin* pour 1770 et 1771. On rencontre, entre autres résultats remarquables, dans ce grand travail, le beau théorème que voici :

Dès qu'on aura trouvé, par un moyen quelconque, la valeur d'une fonction rationnelle des racines d'une équation, on pourra en général trouver la valeur d'une autre fonction rationnelle quelconque des mêmes racines, et cela par le moyen d'une équation simplement linéaire. Quelques cas particuliers exigeront la résolution d'une équation du deuxième, du troisième, etc., degré.

La démonstration de ce théorème et le développement de ses conséquences feront le sujet de cette leçon; mais, pour ne pas interrompre notre exposition, nous commencerons par établir une proposition importante, dont nous aurons besoin.

Théorème sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme.

Soit

$$V = F(a, b, c, \ldots, k, l)$$

une fonction des m lettres $a, b, c, \ldots, k, l$.

Désignons, pour abréger,

$$A_1, A_2, A_3, \ldots, A_M$$

les $M = 1.2\ldots m$ permutations dont ces lettres sont susceptibles, et représentons par la notation

$$\begin{pmatrix} A_\alpha \\ A_\beta \end{pmatrix}$$

l'opération qui consiste à remplacer les lettres de la permutation A_α par celles de même rang dans la permutation A_β : cette opération se nomme une *substitution*.

On obtiendra toutes les valeurs que la fonction V peut prendre par les permutations des lettres a, b, c, etc., en lui appliquant les M substitutions

$$\begin{pmatrix} A_1 \\ A_1 \end{pmatrix}, \begin{pmatrix} A_1 \\ A_2 \end{pmatrix}, \begin{pmatrix} A_1 \\ A_3 \end{pmatrix}, \ldots, \begin{pmatrix} A_1 \\ A_M \end{pmatrix},$$

dont la première est une substitution *identique*. Il en résultera, pour la fonction V, M valeurs que nous désignerons par

$$V_1, V_2, \ldots, V_M.$$

On voit que le nombre des valeurs distinctes de V est au plus égal à M : mais il peut être moindre; cela arrivera, par exemple, si la fonction V est symétrique par rapport à quelques-unes des m lettres a, b, etc.

Il peut arriver aussi qu'une fonction qui n'est symé-

trique par rapport à aucunes lettres, ne puisse pas cependant acquérir M valeurs distinctes. Nous citerons pour exemple la fonction

$$(a-b)(a-c)(b-c),$$

qui ne peut acquérir que deux valeurs, bien qu'elle ne soit symétrique par rapport à aucune des trois lettres qu'elle renferme.

Quand nous disons qu'une substitution change ou ne change pas la valeur d'une fonction, il est bien entendu que nous faisons abstraction des valeurs numériques qu'on peut, ultérieurement, attribuer aux lettres, et que nous ne voulons parler que de la *valeur algébrique* de la fonction. Ainsi la fonction

$$a+2b+3c$$

est changée par la substitution $\begin{pmatrix} a, & b, & c \\ b, & c, & a \end{pmatrix}$, quoique la nouvelle valeur qu'elle prend, savoir

$$b+2c+3a,$$

puisse être égale à la première, si l'on attribue des valeurs convenables aux lettres a, b, c.

Théorème. — *Le nombre des valeurs distinctes que peut prendre une fonction de m lettres, quand on y permute les lettres qu'elle renferme, est toujours un diviseur du produit* $1.2.3...m$.

Supposons que les valeurs de la fonction V,

$$(1) \qquad V_1, V_2, \ldots, V_M,$$

formées comme il vient d'être dit, ne soient pas toutes distinctes, et que le nombre de celles qui sont égales à V_α, par exemple, soit n; que l'on ait, par conséquent, ces n valeurs égales

$$(2) \qquad V_\alpha = V_\beta = V_\gamma = \ldots = V_\omega,$$

qui correspondent respectivement aux permutations

(3) $$A_\alpha,\ A_6,\ A_\gamma,\ \ldots,\ A_\omega,$$

ou, en d'autres termes, qui se déduisent de V_1 par les substitutions

$$\begin{pmatrix}A_1\\A_\alpha\end{pmatrix},\ \begin{pmatrix}A_1\\A_6\end{pmatrix},\ \begin{pmatrix}A_1\\A_\gamma\end{pmatrix},\ \ldots,\ \begin{pmatrix}A_1\\A_\omega\end{pmatrix}.$$

Soient $V_{\alpha'}$ l'une des fonctions (1) qui ne sont pas égales à V_α, $A_{\alpha'}$ la permutation correspondante, en sorte que $V_{\alpha'}$ se déduise de V_1 par la substitution $\begin{pmatrix}A_1\\A_{\alpha'}\end{pmatrix}$, et considérons les n permutations

(4) $$A_{\alpha'},\ A_{6'},\ A_{\gamma'},\ \ldots,\ A_{\omega'},$$

formées de telle sorte que $A_{6'}$, $A_{\gamma'}$, etc., se déduisent de $A_{\alpha'}$ de la même manière que A_6, A_γ, etc., se déduisent de A_α, c'est-à-dire en exécutant les mêmes changements entre les lettres qui occupent les mêmes places. Par exemple, si A_6 se déduit de A_α en remplaçant dans A_α les lettres qui occupent les rangs 1, 2, 3, 4, respectivement par celles qui occupent les rangs 2, 4, 1, 3, de même aussi $A_{6'}$ devra être formée en remplaçant les lettres qui occupent dans $A_{\alpha'}$ les rangs 1, 2, 3, 4, respectivement par celles qui occupent les rangs 2, 4, 1, 3.

Soient aussi

(5) $$V_{\alpha'},\ V_{6'},\ V_{\gamma'},\ \ldots,\ V_{\omega'}$$

les valeurs de V en nombre égal à n, et qui correspondent aux permutations (4), c'est-à-dire qu'on déduit de V_1 par les substitutions

$$\begin{pmatrix}A_1\\A_{\alpha'}\end{pmatrix},\ \begin{pmatrix}A_1\\A_{6'}\end{pmatrix},\ \begin{pmatrix}A_1\\A_{\gamma'}\end{pmatrix},\ \ldots,\ \begin{pmatrix}A_1\\A_{\omega'}\end{pmatrix}.$$

Je dis que les égalités (2) entraîneront nécessairement les suivantes :

$$V_{\alpha'} = V_{6'} = V_{\gamma'} = \ldots = V_{\omega'}.$$

En effet, V_α et V_6 se déduisant de V_1 par les substitutions $\begin{pmatrix} A_1 \\ A_\alpha \end{pmatrix}$, $\begin{pmatrix} A_1 \\ A_6 \end{pmatrix}$, il est évident que V_6 se déduira de V_α par la substitution $\begin{pmatrix} A_\alpha \\ A_6 \end{pmatrix}$; pareillement, $V_{6'}$ se déduira de $V_{\alpha'}$ en appliquant à cette dernière la substitution $\begin{pmatrix} A_{\alpha'} \\ A_{6'} \end{pmatrix}$. Or, par hypothèse, la substitution $\begin{pmatrix} A_\alpha \\ A_6 \end{pmatrix}$ ne produit aucun changement sur V_α, donc la substitution $\begin{pmatrix} A_{\alpha'} \\ A_{6'} \end{pmatrix}$ ne produira aucun changement sur $V_{\alpha'}$, car $V_{\alpha'}$, $A_{\alpha'}$, $A_{6'}$ ne sont autre chose que V_α, A_α, A_6 où l'on a changé la *notation* d'une certaine manière. On a donc $V_{\alpha'} = V_{6'}$, et l'on voit que, pour la même raison, les fonctions (5) seront toutes égales entre elles. D'ailleurs les n fonctions (5) correspondent respectivement aux permutations (4) qui sont évidemment distinctes et différentes des permutations (3); donc elles se trouveront parmi les M fonctions (1), et l'on aura, par suite,

$$M = 2n \quad \text{ou} \quad M > 2n.$$

Si $M > 2n$ et que $V_{\alpha''}$ désigne l'une des valeurs de V distinctes de V_α et de $V_{\alpha'}$, on fera voir, comme précédemment, que la série (1) contient n nouveaux termes

$$V_{\alpha''},\ V_{6''},\ V_{\gamma''}, \ldots,\ V_{\omega''},$$

tous égaux entre eux : on aura, par conséquent,

$$M = 3n \quad \text{ou} \quad M > 3n;$$

et, en poursuivant ce raisonnement, on voit que les M

fonctions de la série (1) se partageront nécessairement en un certain nombre μ de groupes composés chacun de n fonctions égales entre elles : on aura donc

$$M = \mu n, \quad \text{d'où} \quad \mu = \frac{M}{n};$$

le nombre μ des valeurs distinctes de V est donc un diviseur du produit $M = 1.2.3\ldots m$, comme nous l'avions annoncé.

Ce théorème a été démontré, pour la première fois, par Lagrange, dans le Mémoire cité plus haut. Nous avons suivi, dans la démonstration précédente, la marche indiquée par M. Cauchy dans son Mémoire *sur le nombre des valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme*, Mémoire qui fait partie du tome X du *Journal de l'École Polytechnique*.

Des fonctions semblables.

Deux fonctions de m quantités sont dites *semblables* lorsque les substitutions qui changent la valeur de l'une changent aussi la valeur de l'autre, ou, ce qui revient au même, lorsque les substitutions qui laissent l'une d'elles invariable ne produisent non plus aucun changement sur l'autre.

Ainsi, deux fonctions symétriques des m racines d'une équation, sont deux fonctions semblables qui ne peuvent prendre chacune qu'une seule valeur ; et, plus généralement, si

$$x_1, \ x_2, \ \ldots, x_m$$

désignent les m racines d'une équation de degré m, deux fonctions symétriques de n d'entre elles,

$$x_1, \ x_2, \ \ldots, x_n$$

par exemple, seront aussi deux fonctions semblables

des m racines, et chacune d'elles pourra acquérir un nombre de valeurs égal au nombre des combinaisons de m lettres n à n, c'est-à-dire à

$$\frac{m(m-1)\ldots(m-n+1)}{1.2\ldots n}.$$

Nous ne considérons ici que des fonctions rationnelles.

Propriété des fonctions semblables des racines d'une équation.

Deux fonctions semblables des racines d'une équation sont exprimables rationnellement l'une par l'autre, en sorte que si l'on connaît la valeur d'une fonction quelconque des racines, on pourra déterminer la valeur de toutes les fonctions semblables.

Il y a pourtant quelques cas d'exception que nous examinerons en détail.

Soient, en effet,

$$x_1,\ x_2,\ldots,\ x_m$$

les m racines de l'équation

$$(1)\qquad x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0,$$

et

$$V = F(x_1,\ x_2,\ldots,\ x_m),$$
$$y = f(x_1,\ x_2,\ldots,\ x_m),$$

deux fonctions rationnelles et semblables de ces racines dont la première est supposée avoir une valeur connue.

Appliquons simultanément, aux fonctions F et f, toutes les $1.2.3\ldots m$ substitutions possibles; il en résultera pour V un certain nombre μ de valeurs distinctes, que je représente par

$$(2)\qquad V_1,\ V_2,\ldots,\ V_\mu,$$

et pour la fonction semblable y, les μ valeurs correspondantes

(3) $$y_1, y_2, \ldots, y_\mu.$$

On peut former, par la méthode indiquée dans la deuxième leçon, l'équation qui a pour racines les μ valeurs de V : soit

(4) $$V^\mu + P_1 V^{\mu-1} + P_2 V^{\mu-2} + \ldots + P_{\mu-1} V + P_\mu = 0,$$

ou

$$\psi(V) = 0,$$

cette équation, dont les coefficients sont exprimables rationnellement par ceux de l'équation proposée. On pourrait former, de la même manière, l'équation qui a pour racines les μ valeurs de y; mais cette équation ne nous sera pas nécessaire.

Considérons maintenant la fonction

$$V^n y,$$

où n est un nombre entier quelconque; les valeurs que peut prendre cette fonction par les diverses substitutions seront évidemment

$$V_1^n y_1,\ V_2^n y_2,\ V_3^n y_3, \ldots,\ V_\mu^n y_\mu,$$

puisque, généralement, toute substitution qui change V en V_ρ change aussi y en y_ρ, et il suit de là (deuxième leçon) que la quantité

$$V_1^n y_1 + V_2^n y_2 + V_3^n y_3 + \ldots + V_\mu^n y_\mu$$

sera une fonction symétrique des m racines $x_1, x_2, \ldots, x_m$, et pourra, par conséquent, s'exprimer rationnellement en fonction des coefficients p_1, p_2, etc., de l'équation (1),

quel que soit l'entier n. Donnons à n les valeurs successives $0, 1, 2, \ldots, (\mu-1)$, et posons

$$
(5)\quad \begin{cases}
y_1 + y_2 + y_3 + \ldots + y_\mu = t_0, \\
V_1 y_1 + V_2 y_2 + V_3 y_3 + \ldots + V_\mu y_\mu = t_1, \\
V_1^2 y_1 + V_2^2 y_2 + V_3^2 y_3 + \ldots + V_\mu^2 y_\mu = t_2, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
V_1^{\mu-1} y_1 + V_2^{\mu-1} y_2 + V_3^{\mu-1} y_3 + \ldots + V_\mu^{\mu-1} y_\mu = t_{\mu-1}.
\end{cases}
$$

Les seconds membres t_0, t_1, etc., de ces équations sont tous exprimables rationnellement en fonction des coefficients de l'équation proposée et des quantités connues qui entrent dans F et f; on peut donc les considérer comme connus, et si l'on résout les μ équations (5) par rapport à $y_1, y_2, \ldots, y_\mu$, chacune de ces valeurs de y se trouvera exprimée, comme on va voir, en fonction rationnelle de la valeur correspondante de V.

Ajoutons les équations (5), après les avoir multipliées respectivement par les facteurs

$$\lambda_0,\ \lambda_1,\ \lambda_2, \ldots, \lambda_{\mu-2},\ 1,$$

et faisons, pour abréger,

$$(6)\qquad \varphi(V) = V^{\mu-1} + \lambda_{\mu-2} V^{\mu-2} + \ldots + \lambda_1 V + \lambda_0,$$

on aura

$$
(7)\quad \begin{cases}
y_1 \varphi(V_1) + y_2 \varphi(V_2) + \ldots + y_\mu \varphi(V_\mu) \\
= t_0 \lambda_0 + t_1 \lambda_1 + \ldots + t_{\mu-2} \lambda_{\mu-2} + t_{\mu-1},
\end{cases}
$$

et si l'on veut la valeur de y_ρ par exemple, il suffira de déterminer les facteurs λ_0, λ_1, etc., de manière que l'on ait

$$(8)\qquad \varphi(V_1) = 0,\quad \varphi(V_2) = 0, \ldots,\quad \varphi(V_\mu) = 0,$$

excepté $\varphi(V_\rho) = 0$; alors l'équation (7) donnera

$$(9) \qquad y_\rho = \frac{t_0\lambda_0 + t_1\lambda_1 + \ldots + t_{\mu-2}\lambda_{\mu-2} + t_{\mu-1}}{\varphi(V_\rho)},$$

et il ne reste plus qu'à trouver les valeurs de λ_0, λ_1, etc. ; ce que l'on peut faire très-aisément de la manière suivante.

Les équations (8) qui déterminent ces facteurs expriment que l'équation

$$\varphi(V) = 0$$

a pour racines $V_1, V_2, \ldots, V_\mu$, excepté V_ρ ; mais l'équation (4)

$$\psi(V) = 0$$

a ces mêmes racines, y compris V_ρ ; et comme d'ailleurs les plus hautes puissances de V dans $\varphi(V)$ et dans $\psi(V)$ ont pour coefficient l'unité, on aura identiquement

$$\varphi(V) = \frac{\psi(V)}{V - V_\rho},$$

ou, en développant le quotient de $\psi(V)$ par $V - V_\rho$,

$$\varphi(V) = V^{\mu-1} + \begin{array}{l|l|l} P_1 & V^{\mu-2} + P_2 & V^{\mu-3} + \ldots + P_{\mu-1} \\ + V_\rho & \quad + P_1 V_\rho & \quad + P_{\mu-2} V_\rho \\ & \quad + V_\rho^2 & \quad + P_{\mu-3} V_\rho^2 \\ & & \quad \vdots \\ & & \quad + P_1 V_\rho^{\mu-2} \\ & & \quad + V_\rho^{\mu-1}. \end{array}$$

En identifiant cette valeur de $\varphi(V)$ avec celle donnée par l'équation (6), on obtient les valeurs suivantes des fac-

teurs

$$(10)\quad\begin{cases}\lambda_{\mu-2} = P_1 + V_\rho,\\ \lambda_{\mu-3} = P_2 + P_1 V_\rho + V_\rho^2,\\ \lambda_{\mu-4} = P_3 + P_2 V_\rho + P_1 V_\rho^2 + V_\rho^3,\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ \lambda_0\ldots = P_{\mu-1} + P_{\mu-2} V_\rho + \ldots + P_1 V_\rho^{\mu-2} + V_\rho^{\mu-1}.\end{cases}$$

Ces facteurs étant tous exprimés en fonction de V_ρ et des quantités connues, il en sera de même de y_ρ. On peut donner à l'expression de y_ρ une forme très-simple.

En faisant, pour abréger l'écriture,

$$\begin{aligned}T_{\mu-1} &= t_{\mu-1} + P_1 t_{\mu-2} + P_2 t_{\mu-3} + \ldots + P_{\mu-2} t_1 + P_{\mu-1} t_0,\\ T_{\mu-2} &= t_{\mu-2} + P_1 t_{\mu-3} + P_2 t_{\mu-4} + \ldots + P_{\mu-2} t_0,\\ T_{\mu-3} &= t_{\mu-3} + P_1 t_{\mu-4} + \ldots\ldots + P_{\mu-3} t_0,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\\ &\ldots\ldots\ldots\ldots\ldots\ldots\\ T_1 &= t_1 + P_1 t_0,\\ T_0 &= t_0;\end{aligned}$$

le numérateur de la valeur de y_ρ, donné par l'équation (9), sera

$$T_0 V_\rho^{\mu-1} + T_1 V_\rho^{\mu-2} + \ldots + T_{\mu-2} V_\rho + T_{\mu-1},$$

et quant au dénominateur, il est égal à $\varphi(V_\rho)$, c'est-à-dire à la valeur que prend la fraction $\frac{\psi(V)}{V - V_\rho}$ pour $V = V_\rho$: cette valeur est $\psi'(V_\rho)$, ψ' désignant la dérivée de ψ. Or,

$$\psi'(V) = \mu V^{\mu-1} + (\mu-1) P_1 V^{\mu-2} + \ldots + P_{\mu-2};$$

on aura donc la valeur suivante de y_ρ

$$(11)\quad y_\rho = \frac{T_0 V_\rho^{\mu-1} + T_1 V_\rho^{\mu-2} + \ldots + T_{\mu-2} V_\rho + T_{\mu-1}}{\mu V_\rho^{\mu-1} + (\mu-1) P_1 V_\rho^{\mu-2} + \ldots + 2 P_{\mu-2} V_\rho + P_{\mu-1}},$$

ou, en désignant simplement par V l'une quelconque des valeurs V_1, V_2, etc., par y la valeur correspondante de y,

$$(12)\quad y = \frac{T_0 V^{\mu-1} + T_1 V^{\mu-2} + \ldots + T_{\mu-2} V + T_{\mu-1}}{\mu V^{\mu-2} + (\mu-1) P_1 V^{\mu-2} + \ldots + 2 P_{\mu-2} V + P_{\mu-1}},$$

valeur que nous représenterons aussi, pour abréger, par

$$y = \frac{\Theta(V)}{\psi'(V)}.$$

Examen des cas particuliers qui font exception.

D'après ce qui précède, les valeurs de $y_1, y_2, \ldots, y_\mu$ s'exprimeront rationnellement et en fonction de V_1, $V_2, \ldots, V_\mu$, respectivement par les formules

$$(13)\quad y_1 = \frac{\Theta(V_1)}{\psi'(V_1)}, \quad y_2 = \frac{\Theta(V_2)}{\psi'(V_2)}, \ldots, \quad y_\mu = \frac{\Theta(V_\mu)}{\psi'(V_\mu)}.$$

Mais quelques-unes de ces équations seront illusoires si l'équation

$$\psi(V) = 0$$

a des racines égales; elles le seront même toutes si la précédente équation en V n'a que des racines multiples. Toutefois, si V_ρ est une racine simple de l'équation en V, la valeur correspondante y_ρ sera, dans tous les cas, donnée par la formule

$$y_\rho = \frac{\Theta(V_\rho)}{\psi'(V_\rho)}.$$

Les cas d'exception que nous venons de signaler peuvent

évidemment se présenter; car, bien que les fonctions

$$V_1,\ V_2,\ \ldots,\ V_\mu$$

soient distinctes, quant à la forme algébrique, si les quantités x_1, x_2, etc., dont elles dépendent, ont des valeurs déterminées, quelques-unes de ces fonctions peuvent être *numériquement* égales. Alors les équations (5) sont insuffisantes pour déterminer y_1, y_2, etc.

Supposons, par exemple, que $V_2 = V_1$, mais que toutes les autres valeurs de V soient différentes et distinctes de V_1: les inconnues y_1 et y_2 n'entreront dans les équations (5) que combinées entre elles par voie d'addition, et ces équations (5) ne pourront déterminer que

$$(y_1 + y_2),\ y_3,\ y_4,\ \ldots,\ y_\mu,$$

qui sont au nombre de $\mu - 1$; l'une des équations (5) deviendra inutile, et en se bornant aux $\mu - 1$ premières, on aura

$$\begin{aligned}
&(y_1 + y_2) + y_3 + y_4 + \ldots + y_\mu = t_0,\\
&V_1(y_1 + y_2) + V_3 y_3 + \ldots + V_\mu y_\mu = t_1,\\
&V_1^2(y_1 + y_2) + V_3^2 y_3 + \ldots + V_\mu^2 y_\mu = t_2,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&V_1^{\mu-1}(y_1 + y_2) + V_3^{\mu-2} y_3 + \ldots + V_\mu^{\mu-2} y_\mu = t_{\mu-1}.
\end{aligned}$$

En opérant sur ces équations, comme nous avons fait sur les équations (5), on déterminera les inconnues

$$y_1 + y_2,\ y_3,\ \ldots,\ y_\mu,$$

qui se trouveront exprimées respectivement en fonction rationnelle de

$$V_1 \text{ ou } V_2,\ V_3,\ \ldots,\ V_\mu.$$

Et généralement si l'équation

$$\psi(V) = 0$$

a α racines égales à V_1, 6 racines égales à V_2, etc., les équations (5), dont quelques-unes deviendront alors inutiles, ne pourront faire connaître que la somme des α valeurs de y, qui correspondent aux α valeurs de V égales à V_1, en fonction rationnelle de V_1; celle des 6 valeurs de y, qui correspondent aux 6 valeurs de V égales à V_2, en fonction rationnelle de V_2, et ainsi de suite. Voici comment on pourra, dans ce cas, déterminer les valeurs de y.

Supposons qu'on ait ces α valeurs de V égales entre elles,

$$V_1 = V_2 = \ldots = V_\alpha;$$

on pourra calculer, en fonction de V_1, la somme

$$y_1 + y_2 + \ldots + y_\alpha.$$

On pourra aussi calculer, de la même manière, la somme des carrés de ces quantités, la somme de leurs cubes, etc., et enfin la somme de leurs puissances α; on pourra donc former (deuxième leçon) l'équation de degré α, qui a pour racines les quantités $y_1, y_2, \ldots, y_\alpha$. Ainsi, quand l'équation en V a des racines égales, la détermination de la fonction y, semblable à V, peut dépendre d'une équation du second, ou du troisième, ou etc., degré.

On peut former, sans faire de nouveaux calculs, la somme des valeurs de y qui correspondent aux valeurs égales de V, et la déduire des équations (13). Supposons, par exemple, que $V_2 = V_1$, mais que les autres valeurs V_3, V_4, etc., soient différentes de V_1; augmentons les coefficients de l'équation proposée (1) de quantités infiniment petites, de manière que V_2 ne soit plus égal à V_1, et posons $V_2 = V_1 + h$, h étant un infiniment petit: on aura

$$y_1 = \frac{\Theta(V_1)}{\psi'(V_1)}, \qquad y_2 = \frac{\Theta(V_1 + h)}{\psi'(V_1 + h)}.$$

Soit

$$\psi(V) = (V - V_1)(V - V_1 - h)\psi_1(V);$$

on aura, en différentiant,

$$\psi'(V) = (V - V_1)(V - V_1 - h)\psi_1'(V) + [2(V - V_1) - h]\psi_1(V),$$

et, par suite,

$$\psi'(V_1) = -h\psi_1(V_1), \quad \psi'(V_1 + h) = h\psi_1(V_1 + h),$$

ou, en négligeant les puissances de h supérieures à la première dans $\psi'(V_1 + h)$,

$$\psi'(V_1 + h) = h\psi_1(V_1).$$

D'après cela, les valeurs de y_1 et y_2 seront

$$y_1 = \frac{-\Theta(V_1)}{h\psi_1(V_1)}, \quad y_2 = \frac{\Theta(V_1 + h)}{h\psi_1(V_1)};$$

donc

$$y_1 + y_2 = \frac{\Theta(V_1 + h) - \Theta(V_1)}{h\psi_1(V_1)}.$$

Cette équation est inexacte, puisque nous avons négligé les puissances de h supérieures à la première; mais elle sera exacte à la limite, pour $h = 0$, c'est-à-dire quand on égalera à zéro les quantités ajoutées aux coefficients de l'équation proposée. Or, pour $h = 0$, on a

$$\frac{\Theta(V_1 + h) - \Theta(V_1)}{h} = \Theta'(V_1)$$

et

$$\psi_1(V_1) = \lim \frac{\psi(V)}{(V - V_1)^2}, \text{ pour } V = V_1,$$

c'est-à-dire

$$\psi_1(V_1) = \frac{\psi''(V_1)}{2};$$

on aura donc, enfin,

$$\frac{y_1 + y_2}{2} = \frac{\Theta'(V_1)}{\psi''(V_1)},$$

et l'on ferait voir assez aisément que si l'on a, en général,

$$V_1 = V_2 = \ldots = V_\alpha,$$

on aura en même temps

$$(14) \qquad \frac{y_1 + y_2 + \ldots + y_\alpha}{\alpha} = \frac{\Theta^{\alpha-1}(V_1)}{\psi^\alpha(V_1)},$$

en sorte qu'on obtiendra la moyenne arithmétique des valeurs de y qui correspondent aux valeurs de V égales à V_1, en prenant la valeur illusoire de y_1 donnée par les équations (13), et substituant au numérateur et au dénominateur de cette valeur de y_1, leurs dérivées d'ordre $\alpha - 1$ par rapport à V_1. La démonstration de l'équation (14) n'offre aucune difficulté; mais comme cette formule est seulement curieuse, et ne nous sera d'aucune utilité, nous nous bornerons aux développements qui précèdent.

Méthode pour calculer une fonction des racines d'une équation, quand on connaît une autre fonction quelconque des racines

La théorie qui vient d'être exposée peut être aisément étendue au cas où la fonction inconnue y n'est pas semblable à la fonction donnée V.

Nous désignerons toujours par $x_1, x_2, \ldots, x_m$ les m racines de l'équation proposée, et par M le produit $1.2.3\ldots m$. Si l'on applique simultanément aux deux fonctions V et y les M substitutions que l'on peut faire, il en résultera pour V, M valeurs

$$V_1, V_2, V_3, \ldots, V_M,$$

et pour y, M valeurs correspondantes

$$y_1, y_2, y_3, \ldots, y_M;$$

le nombre des valeurs distinctes de V ou de y, s'il n'est pas égal à M, sera un diviseur de M, ainsi que nous l'avons démontré au commencement de cette leçon. Il convient de distinguer deux cas :

1°. Supposons d'abord que les M valeurs de V soient distinctes, algébriquement parlant, ce qui n'empêchera pas que quelques-unes de ces valeurs ne puissent être numériquement égales, et ne faisons d'ailleurs aucune hypothèse sur le nombre des valeurs distinctes de y. Dans ce cas, la méthode précédemment exposée s'appliquera, sans modification, à la détermination de chaque valeur de y en fonction de la valeur correspondante de V. On aura toujours, en conservant nos mêmes notations,

$$y = \frac{T_0 V^{\mu-1} + T_1 V^{\mu-2} + \ldots + T_{\mu-2} V + T_{\mu-1}}{\mu V^{\mu-1} + (\mu-1) P_1 V^{\mu-2} + \ldots + 2 P_{\mu-2} V + P_{\mu-1}} = \frac{\Theta(V)}{\psi'(V)};$$

seulement, on aura ici $\mu = M$, et en donnant à V successivement ses M valeurs, l'équation précédente fera connaître toutes les valeurs de y chacune répétée le même nombre de fois, et exprimée chacune par la valeur de V correspondante. Si l'équation $\psi(V) = 0$ a des racines égales, on opérera identiquement, de la même manière que si V et y étaient fonctions semblables.

2°. Supposons que le nombre des valeurs distinctes de V soit moindre que M : désignons-le par μ, et posons

$$M = n\mu;$$

les M valeurs de V,

$$V_1, \; V_2, \; \ldots, \; V_M,$$

se partageront alors en μ groupes contenant chacun n valeurs égales. Soient

$$\begin{array}{l} V_1, \; V_2, \ldots\ldots\ldots, \; V_n, \\ V_{n+1}, \; V_{n+2}, \ldots\ldots, \; V_{2n}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ V_{(\mu-1)n+1}, \ldots\ldots, \; V_{\mu n}, \end{array}$$

ces μ groupes, et désignons toujours par y_ρ la valeur de y correspondante à V_ρ.

Pour ramener ce cas à celui des fonctions semblables, désignons par z une fonction symétrique et rationnelle quelconque des quantités

$$y_1,\ y_2,\ldots,\ y_n,$$

il est évident que V et z seront des fonctions semblables; on pourra donc exprimer z en fonction rationnelle de V. Quand on aura ainsi calculé n fonctions symétriques des quantités $y_1, y_2, \ldots, y_n$, on pourra former l'équation du degré n, qui a pour racines ces n valeurs de y.

On voit, par ce qui précède, qu'on pourra toujours déterminer les racines $x_1, x_2, \ldots, x_m$ d'une équation donnée, si l'on connaît la valeur d'une fonction V de ces racines; pourvu que les $1.2.3\ldots m$ valeurs que prend cette fonction, quand on y permute les racines, soient différentes, non-seulement sous le rapport de la forme algébrique, mais encore au point de vue numérique.

En effet, on peut supposer que la fonction inconnue y se réduise à l'une quelconque des racines, à x_1 par exemple: alors on pourra exprimer x_1 en fonction rationnelle de V et des coefficients de l'équation proposée: si ensuite on suppose que y se réduise à une autre racine x_2, on pourra de même exprimer x_2 en fonction rationnelle de V, et ainsi de suite. D'où il résulte que si la valeur donnée de V est commensurable, les racines de l'équation proposée seront toutes commensurables.

Mais si la fonction V n'a pas toutes ses valeurs distinctes, que l'on ait, par exemple,

$$V_1 = V_2 = V_3,$$

et si, faisant toujours $y = x_1$, les valeurs de y correspondantes sont

$$x_1,\ x_2,\ x_3,$$

la méthode précédente ne fera plus connaître ces racines, elle permettra seulement de former l'équation du troisième degré, dont elles dépendent.

La théorie qui vient d'être exposée comprend tout ce que l'on sait de plus général sur l'abaissement des équations quand on connaît une relation entre les racines, car ce cas est évidemment le même que celui où l'on donne la valeur d'une fonction des racines.

DOUZIÈME LEÇON.

Application de la théorie exposée dans la leçon précédente. — Nouvelle démonstration d'un théorème établi dans cette leçon.

Application de la théorie exposée dans la leçon précédente.

Quoique la théorie exposée dans la précédente leçon soit très-simple, je ne crois pas inutile de montrer sur un exemple comment les calculs doivent être exécutés.

Nous nous proposerons de calculer l'une des trois racines x_1, x_2, x_3 de l'équation du troisième degré

$$x^3 - 6x^2 + 11x - 6 = 0,$$

x_1 par exemple, sachant que la fonction

$$V = x_1 + 2x_2 - 4x_3$$

est égale à 3.

Faisons

$$y = x_1,$$

et appliquons aux fonctions V et y les $1.2.3 = 6$ substitutions

$$\begin{pmatrix} x_1, x_2, x_3 \\ x_1, x_2, x_3 \end{pmatrix}, \quad \begin{pmatrix} x_1, x_2, x_3 \\ x_1, x_3, x_2 \end{pmatrix}, \quad \begin{pmatrix} x_1, x_2, x_3 \\ x_2, x_3, x_1 \end{pmatrix},$$
$$\begin{pmatrix} x_1, x_2, x_3 \\ x_2, x_1, x_3 \end{pmatrix}, \quad \begin{pmatrix} x_1, x_2, x_3 \\ x_3, x_1, x_2 \end{pmatrix}, \quad \begin{pmatrix} x_1, x_2, x_3 \\ x_3, x_2, x_1 \end{pmatrix};$$

il en résultera les six valeurs suivantes pour V et y :

$$\begin{aligned}
V_1 &= x_1 + 2x_2 - 4x_3, & y_1 &= x_1, \\
V_2 &= x_1 + 2x_3 - 4x_2, & y_2 &= x_1, \\
V_3 &= x_2 + 2x_3 - 4x_1, & y_3 &= x_2, \\
V_4 &= x_2 + 2x_1 - 4x_3, & y_4 &= x_2, \\
V_5 &= x_3 + 2x_1 - 4x_2, & y_5 &= x_3, \\
V_6 &= x_3 + 2x_1 - 4x_1, & y_6 &= x_3.
\end{aligned}$$

On formera l'équation du sixième degré en V,

$$V^6 + P_1 V^5 + P_2 V^4 + P_3 V^3 + P_4 V^2 + P_5 V + P_6 = 0,$$

et l'on trouvera

$$P_1 = 12, \quad P_2 = -2, \quad P_3 = -336,$$
$$P_4 = -287, \quad P_5 = 2052, \quad P_6 = 2016;$$

on calculera ensuite les quantités t_0, t_1, t_2, t_3, t_4, t_5, telles que

$$\sum y \quad = t_0,$$
$$\sum Vy \quad = t_1,$$
$$\sum V^2 y = t_2,$$
$$\sum V^3 y = t_3,$$
$$\sum V^4 y = t_4,$$
$$\sum V^5 y = t_5,$$

par la méthode des fonctions symétriques : on trouvera ainsi

$$t_0 = 12, \quad t_1 = -16, \quad t_2 = 264,$$
$$t_3 = -1240, \quad t_4 = 11592, \quad t_5 = -80296;$$

et en posant, comme précédemment,

$$T_5 = t_5 + P_1 t_4 + P_2 t_3 + P_3 t_2 + P_4 t_1 + P_5 t_0,$$
$$T_4 = t_4 + P_1 t_3 + P_2 t_2 + P_3 t_1 + P_4 t_0,$$
$$T_3 = t_3 + P_1 t_2 + P_2 t_1 + P_3 t_0,$$
$$T_2 = t_2 + P_1 t_1 + P_2 t_0,$$
$$T_1 = t_1 + P_1 t_0,$$
$$T_0 = t_0,$$

on aura

$$T_5 = 1800, \quad T_4 = -1884, \quad T_3 = -2072,$$
$$T_2 = 48, \quad T_1 = 128, \quad T_0 = 12.$$

Maintenant la formule générale

$$y = \frac{T_0 V^5 + T_1 V^4 + T_2 V^3 + T_3 V^2 + T_4 V + T_5}{6 V^5 + 5 P_1 V^4 + 4 P_2 V^3 + 3 P_3 V^2 + 2 P_4 V + P_5},$$

où l'on doit affecter y et V de mêmes indices, devient

$$y = \frac{12 V^5 + 128 V^4 + 48 V^3 - 2072 V^2 - 1884 V + 1800}{6 V^5 + 60 V^4 - 8 V^3 - 1008 V^2 - 574 V + 2052}.$$

Pour avoir la racine x_1, il faudra faire $V = 3$, et l'on trouvera ainsi

$$x_1 = \frac{-7920}{-2640} = 3.$$

On voit, par ce qui précède, que les calculs auxquels conduit notre théorie sont d'une longueur rebutante, même dans les cas les plus simples; mais il ne faut pas oublier que nous nous plaçons au point de vue théorique, bien plutôt qu'à celui de l'application. Toutefois ces calculs se simplifient en suivant une nouvelle marche indiquée par Gallois.

Nouvelle démonstration d'un théorème établi dans la leçon précédente.

THÉORÈME. — *Si*

$$f(x) = 0 \tag{1}$$

est une équation quelconque de degré m, mais qui n'a pas de racines égales, et que

$$V = \varphi(x_1, x_2, \ldots, x_m)$$

soit une fonction rationnelle des racines $x_1, x_2, \ldots, x_m$

de l'équation (1), *tellement choisie, que les* $1.2.3\ldots m$ *valeurs qu'elle prend, quand on y permute les racines, soient toutes différentes; on pourra exprimer les m racines* $x_1, x_2, \ldots, x_m$ *en fonction rationnelle de* V.

Voici comment Gallois démontre ce théorème dans le Mémoire inséré au tome X du *Journal de Mathématiques* de M. Liouville.

Nous désignerons par V_1 la valeur donnée de V, et par

$$V_1, V_2, \ldots, V_\mu$$

les $\mu = 1.2.3\ldots(m-1)$ valeurs que prend V, quand on y permute les $m-1$ racines

$$x_2, x_3, \ldots, x_m,$$

sans changer la place de x_1. On aura alors une équation en V du degré μ, savoir :

$$(2) \qquad (V - V_1)(V - V_2)\ldots(V - V_\mu) = 0,$$

dont les racines V_1, V_2, etc., seront toutes différentes, et dont les coefficients, qui sont des fonctions symétriques des racines $x_2, x_3, \ldots, x_m$ de l'équation

$$\frac{f(x)}{x - x_1} = 0,$$

s'exprimeront rationnellement par les coefficients de cette équation, c'est-à-dire en fonction de x_1 et des coefficients de l'équation proposée (1). Par suite, l'équation (2) pourra être mise sous la forme

$$(3) \qquad F(V, x_1) = 0,$$

F désignant une fonction rationnelle de V et de x_1. Or l'équation (2), ou l'équation (3), est satisfaite pour $V = V_1$; on aura donc identiquement

$$F(V_1, x_1) = 0.$$

D'où il suit que l'équation

$$(4)\qquad F(V_1, x) = 0$$

sera satisfaite pour

$$x = x_1,$$

et, par conséquent, les équations (1) et (4) auront une racine commune x_1. Je dis, de plus, que ces équations ne sauraient avoir d'autre racine commune. Supposons, en effet, que l'équation (4) soit satisfaite pour $x = x_2$, on aura identiquement

$$F(V_1, x_2) = 0;$$

par suite, l'équation

$$(5)\qquad F(V, x_2) = 0$$

sera satisfaite pour $V = V_1$. Or l'équation (5) se déduit de l'équation (3), ou de l'équation (2), en changeant x_1 et x_2 l'un dans l'autre : d'ailleurs, par ce changement, les quantités $V_1, V_2, \ldots, V_\mu$ se changent en d'autres V'_1, $V'_2, \ldots, V'_\mu$, toutes distinctes des premières par hypothèse; l'équation (5) peut donc se mettre sous la forme

$$(V - V'_1)(V - V'_2)\ldots(V - V'_\mu) = 0,$$

et ne saurait avoir V_1 pour racine.

Les équations (1) et (4) n'ayant que la seule racine commune x_1, on déterminera aisément cette racine. Pour cela on cherchera le plus grand commun diviseur entre $f(x)$ et $F(V_1, x)$, et l'on poussera l'opération jusqu'à ce qu'on obtienne un reste du premier degré en x : en égalant à zéro ce reste, on aura une équation qui fera connaître la valeur de x_1,

$$x_1 = \psi(V_1) \quad \text{ou} \quad x_1 = \psi(V);$$

et cette valeur de x_1 sera évidemment rationnelle en V,

car l'opération du plus grand commun diviseur ne peut jamais introduire de radicaux.

On pourrait opérer de même pour trouver les autres racines, et l'on aurait ainsi pour toutes ces racines des expressions rationnelles, telles que

$$x_1 = \psi_1(V), \quad x_2 = \psi_2(V), \ldots, \quad x_m = \psi_m(V).$$

Corollaire I. — L'équation en V du degré $M = 1.2.3\ldots m$, qui a pour racines toutes les M valeurs de V, et dont les coefficients s'expriment rationnellement par ceux de l'équation proposée, jouit d'une propriété assez curieuse: c'est que toutes ses racines peuvent être exprimées rationnellement par l'une quelconque d'entre elles. Soient, en effet, V et V_2 deux des valeurs de V; V_2 est une fonction rationnelle des racines $x_1, x_2, \ldots, x_m$, lesquelles, d'après ce qui précède, sont des fonctions rationnelles de V : on aura donc

$$V_2 = \Theta(V),$$

Θ désignant une fonction rationnelle.

Corollaire II. — On peut aussi déduire, de ce qui précède, la proposition suivante :

Étant données tant d'irrationnelles algébriques qu'on voudra, on peut toujours les exprimer toutes en fonction rationnelle d'une même irrationnelle.

Soient, en effet,

$$x_1, \ x_2, \ldots, \ x_n,$$

n irrationnelles algébriques quelconques; on pourra former une équation d'un certain degré m, à coefficients commensurables, dont ces n quantités seront racines, et qui n'aura pas de racines égales. Soient

$$x_1, \ x_2, \ldots, \ x_m$$

les m racines de cette équation, et désignons par V une

fonction rationnelle de ces m racines telle, que les valeurs qu'elle prend par les substitutions soient toutes distinctes. V sera une irrationnelle algébrique en fonction rationnelle de laquelle les n irrationnelles données pourront s'exprimer, d'après le théorème précédent.

Nous admettons comme évident qu'on peut toujours former une fonction rationnelle de m quantités inégales telle, que les $1.2.3\ldots m$ valeurs qu'on en déduit par les substitutions soient différentes.

Application à un exemple. — Le théorème précédent fournit une méthode beaucoup plus simple que celle qui résulte de la théorie de Lagrange, pour déterminer les racines d'une équation quand on se donne une fonction de ces racines. Nous prendrons comme exemple le cas de l'équation du troisième degré.

Soit l'équation

$$x^3 + p_1 x^2 + p_2 x + p_3 = 0, \tag{1}$$

et posons

$$V = ax_1 + bx_2 + cx_3.$$

En permutant les lettres x_2 et x_3, on aura ces deux valeurs de V,

$$V_1 = ax_1 + bx_2 + cx_3,$$
$$V_2 = ax_1 + bx_3 + cx_2;$$

l'équation en V sera alors

$$(V - V_1)(V - V_2) = 0,$$

ou

$$V^2 - [2ax_1 + (b+c)(x_2 + x_3)]V$$
$$+ [a^2x_1^2 + a(b+c)x_1(x_2+x_3) + bc(x_2^2+x_3^2) + (b^2+c^2)x_2x_3] = 0.$$

On peut chasser x_2 et x_3 de cette équation à l'aide des relations

$$x_2 + x_3 = -p_1 - x_1,$$
$$x_2 x_3 = p_2 - x_1(x_2 + x_3) = p_2 + p_1 x_1 + x_1^2,$$
$$x_2^2 + x_3^2 = (p_1^2 - 2p_2) - x_1^2,$$

et l'on aura

$$(2)\left\{\begin{array}{c} V^2 - [(2a - b - c)x_1 - p_1(b+c)]V \\ + \left[\begin{array}{c}(a^2 + b^2 + c^2 - ab - ac - bc)x_1^2 \\ + (b^2 + c^2 - ab - ac)p_1 x_1 + bc p_1^2 - (b-c)^2 p_2\end{array}\right]\end{array}\right\} = 0.$$

Il faudra maintenant, pour avoir x_1, faire $x = x_1$ dans le premier membre de l'équation (1) et chercher le plus grand commun diviseur entre le polynôme que l'on obtiendra ainsi et le premier membre de l'équation (2) : il n'y a même aucun calcul à faire dans le cas particulier où l'on a

$$a^2 + b^2 + c^2 - ab - ac - bc = 0\,;$$

car alors l'équation (2) ne contient plus que la première puissance de x_1, et fait connaître immédiatement sa valeur. Ce cas simple se présente si l'on prend pour a, b, c les trois racines cubiques de l'unité.

Soit α une racine cubique imaginaire de l'unité, et posons

$$a = 1, \quad b = \alpha, \quad c = \alpha^2,$$

on aura, en remarquant que $\alpha + \alpha^2 + 1 = 0$,

$$x_1 = \frac{V^2 - p_1 V + (p_1^2 - 3p_2)}{3V}.$$

TREIZIÈME LEÇON.

Propriétés des racines de l'équation binôme. Des racines primitives et de leur nombre. — Digression sur la résolution numérique de l'équation à laquelle se ramène l'équation binôme, quand on lui applique la méthode d'abaissement des équations réciproques. Exposition de la méthode de M. Sturm pour la separation des racines.

Les racines de l'unité jouent un rôle important dans la théorie de la résolution algébrique des équations, dont nous allons bientôt nous occuper; je crois donc utile de rappeler ici les propriétés de ces racines, dont quelques-unes sont démontrées dans les Traités élémentaires d'Algèbre.

Propriétés des racines de l'équation binôme. Des racines primitives et de leur nombre.

I. *Les racines communes à deux équations binômes de la forme*

$$x^m = 1, \quad x^n = 1,$$

sont également racines de l'équation

$$x^\theta = 1,$$

où θ désigne le plus grand commun diviseur des nombres m et n.

Supposons, en effet, que l'on ait à la fois

$$\alpha^m = 1 \quad \text{et} \quad \alpha^n = 1;$$

soit $m > n$, et désignons par q le quotient et par r le reste de la division de m par n, en sorte que $m = nq + r$:

on aura

$$\alpha^{nq+r} = 1, \quad \text{ou} \quad \alpha^{nq}.\alpha^r = 1.$$

Mais, à cause de $\alpha^n = 1$, on a aussi $\alpha^{nq} = 1$; donc

$$\alpha^r = 1.$$

D'où l'on conclut aisément que si r, r', r'', ..., θ sont les restes auxquels conduit la recherche du plus grand commun diviseur des entiers m et n, on aura

$$\alpha^r = 1, \ \alpha^{r'} = 1, \ldots, \ \alpha^\theta = 1,$$

et, par conséquent, toute racine commune, α, aux deux équations proposées, est aussi racine de

$$x^\theta = 1.$$

Il est évident d'ailleurs que, réciproquement, les racines de cette dernière équation appartiennent aux deux équations proposées.

Il résulte de là que si m et n sont premiers entre eux, les deux équations

$$x^m = 1, \ x^n = 1$$

n'auront d'autre racine commune que l'unité, et que, si m est un nombre premier, l'équation

$$x^m = 1$$

n'aura de racine commune autre que l'unité, avec aucune équation de degré moindre.

II. *Si α désigne une racine quelconque de l'équation binôme*

$$x^m = 1,$$

toute puissance de α sera aussi racine de la même équation.

L'équation

$$\alpha^m = 1$$

entraîne, en effet,

$$\alpha^{mk} = 1, \quad \text{ou} \quad (\alpha^k)^m = 1,$$

et, par conséquent, tous les termes de la série

$$\alpha,\ \alpha^2,\ \alpha^3,\ldots$$

seront racines de la même équation. Or, à cause de $\alpha^m = 1$, on a aussi

$$\alpha^{m+1} = \alpha,\ \alpha^{m+2} = \alpha^2,\ldots;$$

d'où il suit que la série précédente contiendra au plus, comme cela doit être, m quantités distinctes, savoir :

$$\alpha,\ \alpha^2,\ \alpha^3,\ldots,\ \alpha^{m-1},\ \alpha^m \text{ ou } 1.$$

Si m est un nombre *premier*, et si α n'est pas égal à l'unité, les m termes de la série précédente sont différents ; car si l'on avait, par exemple,

$$\alpha^{n+n'} = \alpha^{n'},$$

n' et $n + n'$ étant inférieurs à m, on aurait, en divisant par $\alpha^{n'}$,

$$\alpha^n = 1;$$

ce qui ne peut être, puisque l'équation $x^m = 1$ ne saurait avoir d'autre racine commune que l'unité avec $x^n = 1$. Il en résulte ce théorème :

Si m est un nombre premier, et α une racine quelconque de l'équation

$$x^m = 1,$$

autre que l'unité, les m racines de cette équation seront représentées par

$$\alpha,\ \alpha^2,\ \alpha^3,\ldots,\ \alpha^{m-1},\ \alpha^m.$$

La proposition précédente n'a plus lieu lorsque m est un nombre composé, et qu'on prend pour α une racine quelconque de

$$x^m = 1;$$

mais elle aura lieu évidemment, d'après ce qui précède, si l'on prend pour α une racine qui n'appartienne en

même temps à aucune équation $x^n = 1$ de degré n inférieur à m.

Cela posé, nous appellerons *racines primitives* de l'équation binôme

$$x^m = 1,$$

les racines de cette équation qui n'appartiennent à aucune équation de degré moindre et de même forme, telle que

$$x^n = 1.$$

Si m est premier, toute racine de $x^m = 1$, autre que 1. est une racine primitive; et, dans tous les cas, chaque racine primitive jouit de la propriété de pouvoir donner toutes les racines par ses diverses puissances.

Nous allons démontrer actuellement l'existence des racines primitives pour toute équation binôme, de degré non premier, et déterminer en même temps le nombre de ces racines primitives.

III. Considérons d'abord le cas où le degré de l'équation binôme

$$x^m = 1$$

est une puissance d'un nombre premier p, et soit

$$m = p^\mu;$$

toute racine non primitive de l'équation

$$x^{p^\mu} = 1$$

doit appartenir à une équation telle que

$$x^\theta = 1,$$

où θ désigne un diviseur de p^μ : mais tout diviseur de p^μ, autre que p^μ lui-même, doit diviser $p^{\mu-1}$; donc les racines de l'équation précédente, et par suite toutes les racines *non primitives* de la proposée, doivent appartenir

à l'équation

$$x^{p^{\mu-1}} = 1.$$

D'ailleurs toutes les racines de cette dernière appartiennent évidemment à la proposée; le nombre des racines non primitives de la proposée est donc $p^{\mu-1}$, et, par conséquent, celui des racines primitives est

$$p^\mu - p^{\mu-1}, \quad \text{ou} \quad p^\mu\left(1-\frac{1}{p}\right), \quad \text{ou} \quad m\left(1-\frac{1}{p}\right).$$

Nous allons maintenant faire connaître la manière dont sont formées les racines primitives.

Considérons toujours l'équation

$$(1) \qquad x^{p^\mu} = 1,$$

et soient $\mathcal{E}_1$ une racine quelconque de l'équation

$$x^p = 1,$$

$\mathcal{E}_2$ une racine quelconque de

$$x^p = \mathcal{E}_1,$$

$\mathcal{E}_3$ une racine quelconque de

$$x^p = \mathcal{E}_2,$$

et ainsi de suite jusqu'à ce qu'on obtienne une dernière équation

$$x^p = \mathcal{E}_{\mu-1},$$

dont nous désignerons par $\mathcal{E}_\mu$ une racine quelconque. Si l'on fait

$$(2) \qquad \alpha = \mathcal{E}_1 \mathcal{E}_2 \ldots \mathcal{E}_{\mu-1} \mathcal{E}_\mu,$$

cette expression de α, qui a p^μ valeurs, puisque $\mathcal{E}_1$ a p valeurs, qu'à chacune d'elles correspondent p valeurs de $\mathcal{E}_2$, etc., donnera précisément les p^μ racines de l'équation (1).

On voit d'abord que les valeurs de α satisfont à l'équation (1), car on a

$$\beta_1^p = 1,\quad \beta_2^{p^2} = 1,\quad \beta_3^{p^3} = 1, \ldots,\quad \beta_{\mu-1}^{p^{\mu-1}} = 1,\quad \beta_\mu^{p^\mu} = 1,$$

et, par suite,

$$\alpha^{p^\mu} = 1.$$

Il suffit donc de démontrer que les p_μ valeurs de α sont distinctes. Supposons que deux de ces valeurs soient égales entre elles, que l'on ait, par exemple,

$$(3)\qquad \beta_1 \beta_2 \beta_3 \ldots \beta_{\mu-1} \beta_\mu = \beta'_1 \beta'_2 \beta'_3 \ldots \beta'_{\mu-1} \beta'_\mu;$$

en élevant cette égalité à la puissance p, et se rappelant que

$$(4)\qquad \begin{cases} \beta_1^p = 1, & \beta_2^p = \beta_1, \ldots, \beta_\mu^p = \beta_{\mu-1}, \\ \beta_1'^p = 1, & \beta_2'^p = \beta'_1, \ldots, \beta_\mu'^p = \beta'_{\mu-1}, \end{cases}$$

on aura

$$(5)\qquad \beta_1 \beta_2 \beta_3 \ldots \beta_{\mu-1} = \beta'_1 \beta'_2 \beta'_3 \ldots \beta'_{\mu-1}.$$

Des égalités (3) et (5) on tire

$$\beta_\mu = \beta'_\mu;$$

en opérant sur l'égalité (5), comme nous venons de faire sur l'égalité (3), on obtiendra

$$\beta_{\mu-1} = \beta'_{\mu-1},$$

et, en continuant ainsi, on arrive à cette conséquence, que l'égalité (3) ne peut exister à moins que les quantités $\beta_1, \beta_2, \ldots, \beta_\mu$ ne soient égales chacune à chacune aux quantités $\beta'_1, \beta'_2, \ldots, \beta'_\mu$. D'où il suit que l'équation (2) donnera effectivement toutes les racines de l'équation (1).

Cherchons maintenant quelles sont celles de ces racines qui sont primitives. Comme nous l'avons déjà remarqué, les racines non primitives de l'équation (1) sont celles qui satisfont à l'équation

$$x^{p^{\mu-1}} = 1.$$

Supposons donc que l'on ait

$$(\theta_1 \theta_2 \theta_3 \ldots \theta_{\mu-1} \theta_\mu)^{p^{\mu-1}} = 1;$$

en supprimant les facteurs égaux à l'unité, cette équation se réduit à

$$(6) \qquad \theta_\mu^{p^{\mu-1}} = 1.$$

Mais des égalités (4) on déduit

$$\theta_\mu^{p^{\mu-1}} = \theta_{\mu-1}^{p^{\mu-2}} = \theta_{\mu-2}^{p^{\mu-3}} = \ldots = \theta_2^p = \theta_1;$$

par suite, l'équation (6) exige que

$$\theta_1 = 1.$$

Par où l'on voit que la valeur de α donnée par l'équation (2) sera une racine primitive ou non primitive de l'équation (1), suivant que θ_1 sera différent de 1 ou égal à 1.

De ce qui précède on peut conclure la proposition suivante :

THÉORÈME. — *La résolution de l'équation binôme $x^m = 1$, dont le degré m est une puissance μ d'un nombre premier p, se ramène à déterminer une racine θ_1 autre que l'unité de l'équation $x^p = 1$, une racine θ_2 quelconque de l'équation $x^p = \theta_1$, puis une racine quelconque θ_3 de $x^p = \theta_2$, etc.*

Car on aura, par ce moyen, une racine primitive de l'équation proposée, laquelle donnera toutes les autres par ses diverses puissances.

IV. Considérons maintenant le cas général où le degré m de l'équation binôme

$$x^m = 1 \tag{1}$$

est un nombre composé quelconque; décomposons ce nombre en ses facteurs premiers, et soit

$$m = p^\mu q^\nu \ldots r^\lambda,$$

$p, q, \ldots, r$ désignant des nombres premiers quelconques inégaux.

Écrivons les équations

$$x^{p^\mu} = 1, \quad x^{q^\nu} = 1, \ldots, x^{r^\lambda} = 1; \tag{2}$$

désignons par β une racine quelconque de la première, par γ une racine quelconque de la seconde, etc., par δ une racine quelconque de la dernière, et posons

$$\alpha = \beta\gamma \ldots \delta. \tag{3}$$

Cette expression de α a m valeurs, puisque $\beta, \gamma, \ldots, \delta$ ont respectivement p^μ, $q^\nu, \ldots, r^\lambda$ valeurs; je dis que ce sont précisément les m racines de l'équation (1).

Il est d'abord évident que la précédente valeur de α satisfait à l'équation (1), car on a

$$\beta^{p^\mu} = 1, \quad \gamma^{q^\nu} = 1, \ldots, \quad \delta^{r^\lambda} = 1,$$

et, par suite,

$$\beta^m = 1, \quad \gamma^m = 1, \ldots, \quad \delta^m = 1;$$

d'où

$$\alpha^m = 1.$$

Il faut prouver maintenant que les m valeurs de α sont différentes. Supposons, en effet, que deux de ces valeurs de α soient égales, que l'on ait, par exemple,

$$\beta'\gamma' \ldots \delta' = \beta''\gamma'' \ldots \delta'';$$

comme les quantités $\beta', \gamma', \ldots, \delta'$ ne sont pas toutes égales respectivement à $\beta'', \gamma'', \ldots, \delta''$, admettons que β' diffère



de $6''$, et élevons l'égalité précédente à la puissance $q^{\nu}\ldots r^{\lambda}$, on aura

$$(6'\gamma'\ldots\delta')^{q^{\nu}\ldots r^{\lambda}} = (6''\gamma''\ldots\delta'')^{q^{\nu}\ldots r^{\lambda}},$$

et en supprimant les facteurs égaux à 1,

$$6'^{q^{\nu}\ldots r^{\lambda}} = 6''^{q^{\nu}\ldots r^{\lambda}};$$

mais $6'$ et $6''$ étant deux racines distinctes de l'équation $x^{p^{\mu}} = 1$, peuvent s'exprimer par deux puissances d'une même racine primitive 6 de cette équation ; posons donc

$$6' = 6^{n+n'}, \quad 6'' = 6^{n'},$$

n' et n étant $< p^{\mu}$. Alors la dernière égalité deviendra

$$6^{(n+n')q^{\nu}\ldots r^{\lambda}} = 6^{n'q^{\nu}\ldots r^{\lambda}},$$

ou, simplement,

$$6^{nq^{\nu}\ldots r^{\lambda}} = 1;$$

d'où il suit que 6 est une racine commune aux deux équations

$$x^{p^{\mu}} = 1, \quad x^{nq^{\nu}\ldots r^{\lambda}} = 1,$$

et satisfait, par conséquent, à l'équation

$$x^{\theta} = 1,$$

θ désignant le plus grand commun diviseur à p^{μ} et $nq^{\nu}\ldots r^{\lambda}$. Mais ce plus grand commun diviseur θ est au plus égal à n, et, par conséquent, inférieur à p^{μ} ; donc, 6 n'est pas, comme nous l'avons supposé, une racine primitive de $x^{p^{\mu}} = 1$.

On voit, par là, que l'équation (3) donnera bien les m racines de l'équation (1).

Je dis maintenant que si $6, \gamma, \ldots, \delta$ désignent des

racines primitives de celles des équations (2) auxquelles elles appartiennent respectivement, la valeur de α donnée par l'équation (3) sera une racine primitive de l'équation (1).

Si, en effet, le contraire a lieu, α satisfera à une équation

$$x^\theta = 1,$$

dont le degré θ est un diviseur de m, et il y aura au moins un facteur premier, parmi ceux de m, qui entrera dans θ un moins grand nombre de fois que dans m: supposons que le facteur premier p soit dans ce cas, θ divisera $p^{\mu-1}q^\nu\ldots r^\lambda$, et, par suite, α sera racine de l'équation

$$(4) \qquad x^{p^{\mu-1}q^\nu\ldots r^\lambda} = 1;$$

on aura donc

$$(6\gamma\ldots\delta)^{p^{\mu-1}q^\nu\ldots r^\lambda} = 1.$$

Mais

$$\gamma^{q^\nu} = 1, \ldots, \delta^{r^\lambda} = 1,$$

donc

$$6^{p^{\mu-1}q^\nu\ldots r^\lambda} = 1;$$

d'où il suit que 6 est racine de l'équation (4); or elle l'est aussi de la première des équations (2), d'ailleurs, le plus grand commun diviseur entre les degrés de ces deux équations est $p^{\mu-1}$; donc 6 sera racine de l'équation

$$x^{p^{\mu-1}} = 1,$$

ce qui est contre l'hypothèse, puisque 6 représente une racine primitive de la première des équations (2).

Il résulte, de là, que si l'on ne prend pour $6, \gamma, \ldots, \delta$ que des racines primitives, de la première, de la seconde, etc., de la dernière des équations (2), l'équation (3) ne représentera que des racines primitives pour

l'équation (1). Il est d'ailleurs facile de voir que si β, ou $\gamma,\ldots$, ou δ n'est pas une racine primitive de celle des équations (2), à laquelle elle appartient, la valeur de α donnée par l'équation (3) ne sera pas non plus une racine primitive de l'équation (1). Supposons, en effet, que β ne soit pas une racine primitive de $x^{p^\mu} = 1$; on aura alors

$$\beta^{p^{\mu-1}} = 1, \quad \gamma^{q^\nu} = 1, \ldots, \quad \delta^{r^\lambda} = 1,$$

et, par suite,

$$(\beta\gamma\ldots\delta)^{p^{\mu-1}q^\nu\ldots r^\lambda} = 1;$$

ce qui montre que α ou $\beta\gamma\ldots\delta$ satisfait à une équation binôme de degré inférieur à m.

On peut maintenant connaître le nombre des racines primitives de l'équation (1). En effet, le nombre des racines primitives β est, comme on l'a vu précédemment, $p^\mu\left(1-\frac{1}{p}\right)$, celui des racines primitives γ est de même $q^\nu\left(1-\frac{1}{q}\right)$, etc., donc le nombre des racines primitives α de l'équation (1) est

$$p^\mu q^\nu \ldots r^\lambda \left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\ldots\left(1-\frac{1}{r}\right),$$

ou

$$m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\ldots\left(1-\frac{1}{r}\right).$$

On peut aussi énoncer la proposition suivante :

Théorème. — *La résolution de l'équation binôme $x^m = 1$, où m est un nombre composé quelconque, se ramène à la résolution des équations de même forme, et qui ont respectivement pour degrés les nombres premiers ou puissances de nombres premiers qui divisent le nombre m.*

V. Soient $\alpha, \beta, \gamma, \ldots, \omega$ les m racines de l'équation

$x^m = 1$, ou

$$x^m - 1 = 0,$$

m étant quelconque. On aura, par les formules de Newton (première leçon), les relations suivantes :

$$\alpha + 6 + \gamma + \ldots\ldots\ldots\ldots + \omega = 0,$$
$$\alpha^2 + 6^2 + \gamma^2 + \ldots\ldots\ldots\ldots + \omega^2 = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\alpha^{m-1} + 6^{m-1} + \gamma^{m-1} + \ldots + \omega^{m-1} = 0,$$
$$\alpha^m + 6^m + \gamma^m + \ldots\ldots\ldots + \omega^m = 1;$$

et, généralement, à cause de $\alpha^{m+k} = \alpha^k$, la somme

$$\alpha^\mu + 6^\mu + \gamma^\mu + \ldots + \omega^\mu$$

sera égale à 1 ou à 0, suivant que μ sera divisible ou non divisible par m.

VI. Quant à l'équation binôme plus générale

$$y^m = a,$$

elle se ramène à la forme

$$x^m = 1,$$

si l'on pose

$$y = x\sqrt[m]{a},$$

$\sqrt[m]{a}$ désignant l'une quelconque des quantités qui ont a pour puissance $m^{\text{ième}}$.

On peut démontrer, à l'égard de ces extractions de racines $m^{\text{ièmes}}$, un théorème tout semblable à celui qui concerne les racines $m^{\text{ièmes}}$ de l'unité, lorsque m est un nombre composé.

Supposons d'abord que m soit le produit de deux nombres premiers entre eux p et q, on aura

$$\sqrt[m]{a} = a^{\frac{1}{pq}};$$

or on peut toujours trouver deux entiers ξ et υ tels, que l'on ait

$$p\xi + q\upsilon = 1,$$

puisque p et q sont premiers entre eux : on aura donc

$$\sqrt[m]{a} = a^{\frac{p\xi + q\upsilon}{pq}} = a^{\frac{\xi}{q}} . a^{\frac{\upsilon}{p}} = \sqrt[q]{a^{\xi}} . \sqrt[p]{a^{\upsilon}}.$$

Ainsi l'extraction d'une racine de degré pq se ramène toujours, lorsque p et q sont premiers entre eux, au produit de deux racines, l'une du degré p, l'autre du degré q.

On a, par exemple, quel que soit a,

$$\sqrt[6]{a} = \sqrt{a} . \sqrt[3]{\frac{1}{a}}.$$

Et, en général, si

$$m = p . q \ldots r,$$

$p, q, \ldots, r$ désignant des nombres quelconques premiers entre eux, deux à deux, on pourra écrire

$$\sqrt[m]{a} = \sqrt[p]{a^{\xi}} . \sqrt[q]{a^{\upsilon}} \ldots \sqrt[r]{a^{\omega}},$$

formule dans laquelle $\xi, \upsilon, \ldots, \omega$ sont des nombres entiers positifs ou négatifs.

Digression sur la résolution numérique de l'équation à laquelle se ramène l'équation binôme, quand on lui applique la méthode d'abaissement des équations réciproques. Exposition de la méthode de M. Sturm, pour la séparation des racines.

J'exposerai ici, à l'occasion des équations binômes, qui viennent de nous occuper, la belle méthode de M. Sturm, pour démontrer la réalité des racines de certaines classes

d'équations, et effectuer ensuite la séparation de ces racines.

Considérons l'équation binôme

$$(1) \qquad x^m - 1 = 0,$$

où m est un nombre impair quelconque $2\mu + 1$. En divisant l'équation (1) par $x - 1$, elle devient

$$(2) \qquad x^{2\mu} + x^{2\mu-1} + \ldots + x^2 + x + 1 = 0;$$

et l'on transforme, comme on sait, cette équation (2), conformément à la méthode des équations réciproques, en une autre du degré μ, en la divisant par x^μ, et posant ensuite

$$x + \frac{1}{x} = z;$$

l'équation (2), divisée par x^μ, devient

$$\left(x^\mu + \frac{1}{x^\mu}\right) + \left(x^{\mu-1} + \frac{1}{x^{\mu-1}}\right) + \ldots + \left(x + \frac{1}{x}\right) + 1 = 0,$$

ou

$$(3) \qquad V_\mu + V_{\mu-1} + \ldots + V_2 + V_1 + 1 = 0,$$

en faisant généralement

$$V_n = x^n + \frac{1}{x^n};$$

on peut exprimer facilement V_2, $V_3, \ldots, V_\mu$, en fonction de z, de la manière suivante :

Si l'on multiplie les deux équations

$$V_{n-1} = x^{n-1} + \frac{1}{x^{n-1}},$$

$$z = x + \frac{1}{x},$$

on a

$$z V_{n-1} = \left(x^n + \frac{1}{x^n}\right) + \left(x^{n-2} + \frac{1}{x^{n-2}}\right) = V_n + V_{n-2},$$

d'où

$$(4) \qquad V_n = z V_{n-1} - V_{n-2}.$$

Cette relation fait connaître la valeur de chaque fonction V_n en z, quand on connaît les deux précédentes. Or les deux premières V_0 et V_1 sont connues : on a

$$V_1 = x + \frac{1}{x} = z, \qquad V_0 = x^0 + \frac{1}{x^0} = 2;$$

l'équation (4) permettra donc de calculer les valeurs des fonctions V_2, V_3, etc.

On trouve ainsi

$$(5) \quad \begin{cases} V_0 = 2, \\ V_1 = z, \\ V_2 = z^2 - 2, \\ V_3 = z^3 - 3z, \\ V_4 = z^4 - 4z^2 + 2, \\ V_5 = z^5 - 5z^3 + 5z, \\ V_6 = z^6 - 6z^4 + 9z^2 - 2, \\ \dots\dots\dots\dots \\ \dots\dots\dots\dots \end{cases}$$

Il serait assez difficile de déduire de ces formules l'expression générale de V_n. Nous donnerons, dans la prochaine leçon, le moyen de former cette expression, et nous nous bornerons pour le moment aux remarques suivantes :

1°. V_n est un polynôme du degré n en z, qui ne renferme que des puissances de z de même parité que n;

2°. Les deux premiers termes de V_n sont $z^n - nz^{n-2}$.

En effet, l'équation (4) fait voir que si V_{n-1} et V_{n-2} satisfont à ces conditions, V_n y satisfera également, et l'on voit, à l'inspection des équations (5), que V_2, V_3, V_4, V_5 et V_6 y satisfont, d'où l'on conclut aisément la démonstration.

Posons maintenant

$$U_n = V_n + V_{n-1} + \ldots + V_2 + V_1 + 1; \tag{6}$$

U_n sera un polynôme du degré n en z, et l'équation (3), à laquelle nous avons ramené l'équation (1) sera,

$$U_\mu = 0.$$

Les fonctions U_n sont susceptibles d'un mode de formation identique à celui des fonctions V_n, c'est-à-dire que l'on a

$$U_n = zU_{n-1} - U_{n-2}.$$

En effet, on a, par l'équation (4),

$$V_n = zV_{n-1} - V_{n-2},$$
$$V_{n-1} = zV_{n-2} - V_{n-3},$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$V_2 = zV_1 - 2;$$

en ajoutant ces équations, et ayant égard à l'équation (6), il vient

$$U_n - V_1 - 1 = z(U_{n-1} - 1) - (U_{n-2} + 1);$$

et comme $V_1 = z$,

$$U_n = zU_{n-1} - U_{n-2}, \tag{7}$$

équation qui se déduit de (4), en remplaçant la lettre V par U.

Comme on a

$$U_0 = 1, \quad U_1 = V_1 + 1 = z + 1,$$

l'équation (7) donnera successivement les valeurs des fonctions U_2, U_3, etc. ; on trouve ainsi

$$U_0 = 1,$$
$$U_1 = z + 1,$$
$$U_2 = z^2 + z - 1,$$
$$U_3 = z^3 + z^2 - 2z - 1,$$
....

Quant à l'expression générale de U_n, elle se déduit très-aisément de celle de V_n, ainsi que nous le verrons dans la prochaine leçon.

Nous allons à présent démontrer, d'après M. Sturm, la réalité des racines des équations

$$V_\mu = 0, \quad U_\mu = 0,$$

et indiquer, en même temps, le moyen de séparer ces racines.

De l'équation $V_\mu = 0$. — Nous nous occuperons d'abord de l'équation

$$(1) \qquad V_\mu = 0.$$

Considérons, avec M. Sturm, la suite des fonctions

$$V_\mu,\ V_{\mu-1},\ V_{\mu-2},\ldots,\ V_2,\ V_1,\ V_0,$$

dont la dernière V_0 est constante et égale à 2. Trois fonctions consécutives V_n, V_{n-1}, V_{n-2} sont liées entre elles par l'équation

$$(2) \qquad V_n = zV_{n-1} - V_{n-2};$$

d'où il suit :

1°. Que deux fonctions consécutives V_n et V_{n-1} ne peuvent s'annuler, pour une même valeur de z, puisqu'alors toutes les fonctions suivantes devraient également s'annuler pour la même valeur de z ; ce qui est impossible, la dernière étant constante.

2°. Que si une fonction V_{n-1} s'annule, pour une certaine valeur de z, celle qui la précède et celle qui la suit ont des signes contraires.

Il résulte de là que si l'on fait varier z depuis α jusqu'à 6, la suite des signes des fonctions V ne pourra perdre ni gagner de variations, que lorsque z passera par une valeur annulant V_μ; et que si la suite des signes des fonctions V perd ou gagne k variations quand z varie de α jusqu'à 6, l'équation (1) a *au moins* k racines comprises entre α et 6.

Cela posé, on déduit aisément de l'équation (2), que l'on a pour $z = -2$,

$$V_0 = +2,\quad V_1 = -2,\quad V_2 = +2,\quad V_3 = -2,\ldots,$$

et, pour $z = +2$,

$$V_0 = +2,\quad V_1 = +2,\quad V_2 = +2,\quad V_3 = +2,\ldots;$$

en sorte que la suite des signes des fonctions V perd μ variations quand z varie de -2 jusqu'à $+2$; d'où il suit que l'équation (1) a ses μ racines réelles et comprises entre -2 et $+2$.

En outre, à cause que toutes les racines sont réelles, la suite des signes des fonctions V perdra effectivement une variation chaque fois que z, variant de -2 jusqu'à $+2$, dépassera une racine de l'équation (1), et cette variation se perdra entre les deux premiers termes de la suite, de manière que $V_{\mu-1}$ jouera, par rapport à V_μ, le même rôle que si elle en était la dérivée; ce qui veut dire que les racines de $V_{\mu-1} = 0$ pourront servir à la séparation des racines de $V_\mu = 0$. Enfin, si α et 6 sont deux nombres quelconques compris entre -2 et $+2$, l'équation proposée aura autant de racines entre α et 6, qu'il y a d'unités dans l'excès du nombre des variations de signes de la suite des fonctions V pour $z = \alpha$, sur le nombre des variations de signes de cette suite pour $z = 6$.

De l'équation $U_\mu = 0$. — Ce qui précède s'applique textuellement à l'équation

$$U_\mu = 0,$$

qui se trouve dans les mêmes conditions que l'équation $V^\mu = 0$.

Si l'on considère la suite des fonctions

$$U_\mu,\ U_{\mu-1},\ U_{\mu-2},\ldots,\ U_2,\ U_1,\ U_0,$$

on voit que la dernière est constante, et l'équation

$$U_n = zU_{n-1} - U_{n-2}$$

conduit facilement à cette conséquence, que la suite des signes des fonctions U ne peut perdre ou gagner de variations quand on fait varier z, que lorsque z atteint et dépasse une valeur qui annule la première de ces fonctions; d'où il suit que l'équation proposée a au moins autant de racines entre α et β qu'il y a de variations perdues ou gagnées dans la suite des signes des fonctions U, quand z varie de α à β.

On trouve, d'ailleurs, que pour $z = -2$, la suite des signes des fonctions U présente μ variations, tandis qu'elle n'en présente aucune pour $z = +2$; d'où l'on conclut que l'équation $U_\mu = 0$ a ses μ racines réelles et comprises entre -2 et $+2$.

On démontre très-simplement, dans les cours d'algèbre élémentaire, la réalité des racines des équations que nous venons de considérer; mais j'ai cru devoir présenter ici la méthode de M. Sturm, parce qu'elle s'applique avec succès dans un grand nombre de cas.

QUATORZIÈME LEÇON.

Formation d'une équation différentielle linéaire du deuxième ordre, à laquelle satisfait la fonction V_n. — Expression du polynôme V_n. — Expressions de $\cos na$ et de $\frac{\sin na}{\sin a}$ en fonction de $\cos a$. — Expression du polynôme U_n. — Propriété des racines de l'équation $U_\mu = 0$. — Formation d'une équation différentielle linéaire du deuxième ordre, à laquelle satisfait la fonction U_n. — Nouvelle manière de démontrer la réalité des racines des équations $V_n = 0$, $U_n = 0$.

Je présenterai dans cette leçon quelques développements sur les polynômes V_n et U_n, auxquels nous a conduit la considération de l'équation binôme.

Formation d'une équation différentielle linéaire du deuxième ordre, à laquelle satisfait la fonction V_n.

V_n est une fonction entière d'une variable z. On a

$$V_n = x^n + \frac{1}{x^n}, \tag{1}$$

et

$$z = x + \frac{1}{x}, \tag{2}$$

d'où

$$\frac{dz}{dx} = 1 - \frac{1}{x^2}. \tag{3}$$

Différentions l'équation (1) par rapport à x, il vient

$$\frac{dV_n}{dz}\frac{dz}{dx} = \frac{dV_n}{dz}\left(1 - \frac{1}{x^2}\right) = n\left(x^{n-1} - \frac{1}{x^{n+1}}\right),$$

ou

$$\left(x - \frac{1}{x}\right)\frac{dV_n}{dz} = n\left(x^n - \frac{1}{x^n}\right); \tag{4}$$

différentions aussi cette équation (4) par rapport à x, il vient

$$\left(x-\frac{1}{x}\right)\left(1-\frac{1}{x^2}\right)\frac{d^2V_n}{dz^2}+\left(1+\frac{1}{x^2}\right)\frac{dV_n}{dz}=n^2\left(x^{n-1}+\frac{1}{x^{n+1}}\right),$$

ou

$$(5)\quad \left(x-\frac{1}{x}\right)^2\frac{d^2V_n}{dz^2}+\left(x+\frac{1}{x}\right)\frac{dV_n}{dz}-n^2\left(x^n+\frac{1}{x^n}\right)=0;$$

mais on a

$$x^n+\frac{1}{x^n}=V_n,\quad x+\frac{1}{x}=z,\quad \left(x-\frac{1}{x}\right)^2=z^2-4;$$

donc l'équation (5) devient

$$(6)\qquad (z^2-4)\frac{d^2V_n}{dz^2}+z\frac{dV_n}{dz}-n^2V_n=0.$$

C'est l'équation différentielle que nous voulions obtenir, et qui nous servira à déterminer l'expression du polynôme V_n. Mais il est important pour cette recherche d'établir que V_n, ou le produit de V_n par une constante arbitraire, est la seule fonction entière et rationnelle de z qui puisse satisfaire à l'équation (6). On y parvient aisément de la manière suivante.

Considérons, au lieu de V_n, la fonction plus générale

$$(7)\qquad \Theta_n=Ax^n+\frac{B}{x^n},$$

où A et B sont deux constantes arbitraires. En opérant sur Θ_n, comme nous venons de faire sur V_n, on arrivera à l'équation différentielle

$$(8)\qquad (z^2-4)\frac{d^2\Theta_n}{dz^2}+z\frac{d\Theta_n}{dz}-n^2\Theta_n=0,$$

qui ne diffère de (6) qu'en ce que V_n y est remplacé par Θ_n.

Cette équation (8) a évidemment pour intégrale générale l'équation (7) que l'on peut mettre sous la forme

$$\Theta_n = C\left(x^n + \frac{1}{x^n}\right) + nC'\left(x^n - \frac{1}{x^n}\right),$$

en désignant par C et C' deux constantes arbitraires.

D'ailleurs $x^n + \frac{1}{x^n}$ est précisément V_n, et l'équation (4) donne

$$x^n - \frac{1}{x^n} = \frac{1}{n}\left(x - \frac{1}{x}\right)\frac{dV_n}{dz} = \frac{1}{n}\sqrt{z^2-4}\,\frac{dV_n}{dz};$$

d'où il résulte que l'intégrale générale de l'équation (8) sera

$$\Theta_n = CV_n + C'\sqrt{z^2-4}\,\frac{dV_n}{dz},$$

C et C' étant les deux constantes arbitraires; et, par conséquent, le produit de V_n par une constante C est la fonction rationnelle la plus générale qui puisse satisfaire à l'équation (8).

Expression du polynôme V_n.

Nous savons que V_n est un polynôme du degré n en z, qui ne renferme que des termes de même parité que n; nous savons aussi que le terme du plus haut degré a pour coefficient l'unité. Nous poserons donc

$$(1)\quad V_n = z^n + A_1 z^{n-2} + A_2 z^{n-4} + \ldots + A_{p-1} z^{n-2p+2} + A_p z^{n-2p} + \ldots,$$

et nous allons chercher à déterminer les coefficients A_1, A_2, etc., par la condition que V_n satisfasse à l'équation différentielle

$$(2)\qquad (z^2-4)\frac{d^2V_n}{dz^2} + z\frac{dV_n}{dz} - n^2V_n = 0.$$

Différentions deux fois de suite l'équation (1), on aura

$$\frac{dV_n}{dz} = nz^{n-1} + \ldots + (n-2p)\,A_p\,z^{n-2p-1} + \ldots,$$

$$\frac{d^2V_n}{dz^2} = n(n-1)z^{n-2} + \ldots + (n-2p+2)(n-2p+1)\,A_{p-1}\,z^{n-2p} + (n-2p)(n-2p-1)\,A_p\,z^{n-2p-2} + \ldots,$$

et, en substituant dans l'équation (2) les valeurs de V_n, $\frac{dV_n}{dz}$, $\frac{d^2V_n}{dz^2}$, le coefficient de z^{n-2p} sera

$$\left.\begin{array}{r}(n-2p)(n-2p-1)\\ +(n-2p)\\ -n^2\end{array}\right| A_p - 4(n-2p+2)(n-2p+1)A_{p-1}$$

ou

$$-4p(n-p)A_p - 4(n-2p+2)(n-2p+1)A_{p-1};$$

mais ce coefficient doit être nul, on aura donc

$$A_p = -\frac{(n-2p+2)(n-2p+1)}{p(n-p)}A_{p-1}.$$

Cette relation conduit aisément à l'expression générale de A_p; car, le coefficient A_0 de z^n étant égal à 1, on aura

$$A_p = -\frac{(n-2p+2)(n-2p+1)}{p(n-p)}A_{p-1},$$

$$A_{p-1} = -\frac{(n-2p+4)(n-2p+3)}{(p-1)(n-p+1)}A_{p-2},$$

....

$$A_2 = -\frac{(n-2)(n-3)}{2.(n-2)}A_1,$$

$$A_1 = -\frac{n(n-1)}{1.(n-1)}.$$

En multipliant toutes ces équations, et supprimant les

facteurs communs, il vient

$$A_p = (-1)^p \frac{n(n-p-1)(n-p-2)\ldots(n-2p+2)(n-2p+1)}{1.2.3\ldots p};$$

la valeur du polynôme V_n est donc

$$(3) \left\{\begin{aligned} V_n &= z^n - nz^{n-2} + \frac{n(n-3)}{1.2} z^{n-4} - \frac{n(n-4)(n-5)}{1.2.3} z^{n-6} + \ldots \\ &+ (-1)^p \frac{n(n-p-1)(n-p-2)\ldots(n-2p+2)(n-2p+1)}{1.2\ 3\ldots p} z^{n-2p} + \ldots \end{aligned}\right.$$

Expressions de $\cos na$ *et* $\dfrac{\sin na}{\sin a}$ *en fonction de* $\cos a$.

Le problème que nous venons de résoudre est identique à celui qui a pour objet de trouver l'expression de $\cos na$ en fonction de $\cos a$. Si, en effet, on pose

$$x = \cos a + \sqrt{-1}\sin a,$$

on a

$$z = 2\cos a, \quad V_n = 2\cos na.$$

Exprimer V_n en fonction de z, c'est donc exprimer $\cos na$ en fonction de $\cos a$. En remplaçant V_n et z par $2\cos na$, et $2\cos a$ dans l'équation que nous avons trouvée, il vient

$$(1) \left\{\begin{aligned} \cos na &= 2^{n-1}\cos^n a - 2^{n-3} n \cos^{n-2} a + 2^{n-5}\frac{n(n-3)}{1.2}\cos^{n-4} a - \ldots \\ &+ (-1)^p 2^{n-2p-1} \frac{n(n-p-1)(n-p-2)\ldots(n-2p+1)}{1.2.3\ldots p} \cos^{n-2p} a. \end{aligned}\right.$$

$\sin na$ n'est pas exprimable en fonction rationnelle de $\cos a$, mais le rapport $\dfrac{\sin na}{\sin a}$ l'est. En différentiant l'équation précédente par rapport à a, et divisant ensuite par $-n\sin a$, on a

$$(2) \left\{\begin{aligned} \frac{\sin na}{\sin a} &= 2^{n-1}\cos^{n-1} a - 2^{n-3}(n-2)\cos^{n-3} a + 2^{n-5}\frac{(n-3)(n-4)}{1\ 2}\cos^{n-5} a - \ldots \\ &+ (-1)^p 2^{n-2p-1}\frac{(n-p-1)(n-p-2)\ldots(n-2p+1)(n-2p)}{1.2.3\ \ldots p}\cos^{n-2p-1} a + \ldots \end{aligned}\right.$$

Enfin, en changeant a en $\frac{\pi}{2} - a$ dans les équations (1) et (2), on aura deux autres formules, qui feront connaître, en fonction rationnelle de $\sin a$, $\cos na$ et $\frac{\sin na}{\cos a}$ si n est pair, $\frac{\cos na}{\cos a}$ et $\sin na$ si n est impair.

Expression du polynôme U_n.

Le polynôme que nous avons désigné par U_n a pour valeur

$$U_n = V_n + V_{n-1} + \ldots + V_2 + V_1 + 1,$$

ou

$$U_n = \left(x^n + \frac{1}{x^n}\right) + \left(x^{n-1} + \frac{1}{x^{n-1}}\right) + \ldots + \left(x + \frac{1}{x}\right) + 1.$$

Nous avons trouvé, en différentiant V_n,

$$\left(x - \frac{1}{x}\right)\frac{dV_n}{dz} = n\left(x^n - \frac{1}{x^n}\right),$$

on déduit de là

$$\frac{1}{n}\frac{dV_n}{dz} = \frac{x^n - \frac{1}{x^n}}{x - \frac{1}{x}} = x^{n-1} + x^{n-3} + x^{n-5} + \ldots + \frac{1}{x^{n-3}} + \frac{1}{x^{n-1}};$$

on aurait de même

$$\frac{1}{n+1}\frac{dV_{n+1}}{dz} = x^n + x^{n-2} + x^{n-4} + \ldots + \frac{1}{x^{n-4}} + \frac{1}{x^{n-2}} + \frac{1}{x^n},$$

et, par suite,

$$\frac{1}{n}\frac{dV_n}{dz} + \frac{1}{n+1}\frac{dV_{n+1}}{dz} = x^n + x^{n-1} + \ldots + \frac{1}{x^{n-1}} + \frac{1}{x^n};$$

mais le second membre de cette équation est précisément

égal à U_n, donc

$$U_n = \frac{1}{n}\frac{dV_n}{dz} + \frac{1}{n+1}\frac{dV_{n+1}}{dz}.$$

De l'expression précédemment trouvée pour V_n, on tire

$$\frac{1}{n}\frac{dV_n}{dz} = z^{n-1} - (n-2)z^{n-3} + \frac{(n-3)(n-4)}{1.2}z^{n-5} - \ldots;$$

on a aussi, en changeant n en $n+1$,

$$\frac{1}{n+1}\frac{dV_{n+1}}{dz} = z^n - (n-1)z^{n-2} + \frac{(n-2)(n-3)}{1.2}z^{n-4} - \ldots.$$

Par suite, la valeur de U_n sera

$$\begin{aligned} U_n = z^n + z^{n-1} - (n-1)z^{n-2} - (n-2)z^{n-3} + \frac{(n-2)(n-3)}{1.2}z^{n-4} \\ + \frac{(n-3)(n-4)}{1.2}z^{n-5} - \ldots + (-1)^p\frac{(n-p)\ldots(n-2p+1)}{1.2\ldots p}z^{n-2p} \\ + (-1)^p\frac{(n-p-1)\ldots(n-2p)}{1.2\ldots p}z^{n-2p-1} + \ldots. \end{aligned}$$

Dans cette expression, les termes de même parité que n proviennent tous de $\frac{dV_{n+1}}{dz}$, les autres proviennent de $\frac{dV_n}{dz}$.

Propriété des racines de l'équation $U_\mu = 0$.

Si l'on considère l'équation

$$(1) \qquad x^{2\mu+1} - 1 = 0,$$

puis, qu'après avoir enlevé la racine 1, et divisé par x^μ, on fasse $x + \frac{1}{x} = z$, on a, comme nous l'avons vu, l'équation de degré μ en z,

$$(2) \qquad U_\mu = 0.$$

Soit α une racine primitive de l'équation (1), les 2μ racines imaginaires seront

$$\alpha,\ \alpha^2,\ \alpha^3,\ldots,\ \alpha^{2\mu-1},\ \alpha^{2\mu}.$$

D'ailleurs deux termes de cette suite, également distants des extrêmes, étant évidemment réciproques, les μ racines de l'équation (2) seront

$$\alpha+\frac{1}{\alpha},\quad \alpha^2+\frac{1}{\alpha^2},\ldots,\quad \alpha^{\mu-1}+\frac{1}{\alpha^{\mu-1}},\quad \alpha^{\mu}+\frac{1}{\alpha^{\mu}},$$

ou, en faisant

$$\alpha+\frac{1}{\alpha}=a,$$

et désignant par A_n la valeur de V_n pour $z=a$,

$$a,\ A_2,\ A_3,\ldots,\ A_{\mu}.$$

Ainsi les racines de l'équation (2) sont des fonctions rationnelles de l'une d'entre elles, et même de l'une quelconque d'entre elles, si $2\mu+1$ est un nombre premier. C'est sur cette propriété que M. Gauss a fondé, comme nous le verrons plus tard, une méthode remarquable pour effectuer la résolution de l'équation $U_\mu=0$, lorsque $2\mu+1$ est un nombre premier, cas auquel on ramène tous les autres, ainsi que nous l'avons vu dans la dernière leçon.

Formation d'une équation différentielle linéaire du deuxième ordre, à laquelle satisfait la fonction U_n.

On pourrait employer, pour déterminer le polynôme U_n, un procédé semblable à celui dont nous nous sommes servi pour calculer V_n; on formerait ainsi une équation différentielle à laquelle satisferait U_n, et dont on déduirait ensuite la valeur de ce polynôme; cette seconde

marche, que je me borne à indiquer, est beaucoup moins simple que celle que nous avons suivie, mais l'équation différentielle dont nous venons de parler est utile à connaître. Voici, je crois, le moyen le plus aisé de la trouver.

On a

$$U_n = \left(x^n + \frac{1}{x^n}\right) + \left(x^{n-1} + \frac{1}{x^{n-1}}\right) + \ldots + \left(x + \frac{1}{x}\right) + 1,$$

d'où, en différentiant par rapport à x, se rappelant que $\frac{dz}{dx} = 1 - \frac{1}{x^2}$, et multipliant ensuite par x,

$$\left(x - \frac{1}{x}\right)\frac{dU_n}{dz} = n\left(x^n - \frac{1}{x^n}\right) + (n-1)\left(x^{n-1} - \frac{1}{x^{n-1}}\right) + \ldots + \left(x - \frac{1}{x}\right) + 1;$$

multipliant par $x - \frac{1}{x}$, et observant que

$$\left(x - \frac{1}{x}\right)^2 = z^2 - 4, \quad \text{et} \quad \left(x^p - \frac{1}{x^p}\right)\left(x - \frac{1}{x}\right) = V_{p+1} - V_{p-1},$$

il vient

$$\begin{aligned}(z^2 - 4)\frac{dU_n}{dz} &= n(V_{n+1} - V_{n-1}) + (n-1)(V_n - V_{n-2}) + \ldots \\ &\quad + 3(V_4 - V_2) + 2(V_3 - V_1) + (V_2 - 2), \\ &= nV_{n+1} + (n+1)V_n - 2(V_n + V_{n-1} + \ldots + V_2 + V_1 + 1),\end{aligned}$$

ou

$$(z^2 - 4)\frac{dU_n}{dz} + 2U_n = nV_{n+1} + (n+1)V_n.$$

Différentiant cette équation par rapport à z, on a

$$(z^2 - 4)\frac{d^2U_n}{dz^2} + 2(z+1)\frac{dU_n}{dz} = n(n+1)\left(\frac{1}{n}\frac{dV_n}{dz} + \frac{1}{n+1}\frac{dV_{n+1}}{dz}\right).$$

Mais nous avons déjà trouvé

$$U_n = \frac{1}{n}\frac{dV_n}{dz} + \frac{1}{n+1}\frac{dV_{n+1}}{dz};$$

on a donc enfin

$$(1)\quad (z^2-4)\frac{d^2 U_n}{dz^2}+2(z+1)\frac{dU_n}{dz}-n(n+1)U_n=0.$$

C'est l'équation différentielle que nous voulions former.

Il suit de là que l'équation

$$(2)\quad (z^2-4)\frac{d^2\Theta_n}{dz^2}+2(z+1)\frac{d\Theta_n}{dz}-n(n+1)\Theta_n=0,$$

est satisfaite par

$$\Theta_n=U_n \quad \text{ou} \quad \Theta_n=CU_n,$$

C désignant une constante arbitraire; et cette solution CU_n est la seule solution rationnelle de l'équation (2). On s'en assure aisément en cherchant l'intégrale générale de l'équation (2), ce qui n'a aucune difficulté, du moment qu'on se donne la solution particulière CU_n. On trouve ainsi, pour l'intégrale générale de l'équation (2),

$$\Theta_n=CU_n+C'\sqrt{\frac{z+2}{z-2}}\left[U_n+2(z-2)\frac{dU_n}{dz}\right],$$

C et C′ désignant deux constantes arbitraires; et l'on voit que cette valeur de Θ_n n'est rationnelle que si l'on fait $C'=0$, auquel cas elle se réduit à CU_n.

Nouvelle manière de démontrer la réalité des racines des équations $V_n=0$, $U_n=0$.

Les deux équations différentielles que nous avons formées, et auxquelles satisfont les fonctions V_n et U_n, permettent de démontrer la réalité des racines des équations

$$V_n=0,\quad U_n=0.$$

Cette remarque est importante, car un procédé analogue pourra être employé dans beaucoup d'autres cas. Nous ne nous occuperons que de l'équation $V_n=0$; les mêmes considérations s'appliqueraient à l'équation $U_n=0$.

Nous avons trouvé l'équation différentielle

$$(1) \qquad (z^2-4)\frac{d^2 V_n}{dz^2} + z\frac{dV_n}{dz} - V_n = 0;$$

différentions $p-2$ fois cette équation, et observons que

$$\frac{d^{p-2}}{dz^{p-2}}(z^2-4)\frac{d^2V_n}{dz^2} = (z^2-4)\frac{d^pV_n}{dz^p} + 2(p-2)z\frac{d^{p-1}V_n}{dz^{p-1}} + (p-2)(p-3)\frac{d^{p-2}V_n}{dz^{p-2}},$$

$$\frac{d^{p-2}}{dz^{p-2}} z\frac{dV_n}{dz} = z\frac{d^{p-1}V_n}{dz^{p-1}} + (p-2)\frac{d^{p-2}V_n}{dz^{p-2}}:$$

on aura

$$(2) \qquad \left\{ \begin{aligned} &(z^2-4)\frac{d^pV_n}{dz^p} + (2p-3)z\frac{d^{p-1}V_n}{dz^{p-1}} \\ &\qquad - [n^2-(p-2)^2]\frac{d^{p-2}V_n}{dz^{p-2}} = 0. \end{aligned} \right.$$

Les équations (1) et (2) peuvent s'écrire ainsi :

$$(3) \qquad \left\{ \begin{aligned} &V_n = z\frac{dV_n}{dz} - (4-z^2)\frac{d^2V_n}{dz^2}, \\ &\frac{d^{p-2}V_n}{dz^{p-2}} = \frac{2p-3}{n^2-(p-2)^2} z\frac{d^{p-1}V_n}{dz^{p-1}} - \frac{4-z^2}{n^2-(p-2)^2}\frac{d^pV_n}{dz^p}. \end{aligned} \right.$$

Cela posé, considérons la suite formée de la fonction V_n et de toutes ses dérivées

$$(4) \qquad V_n, \quad \frac{dV_n}{dz}, \quad \frac{d^2V_n}{dz^2}, \ldots, \quad \frac{d^nV_n}{dz^n}:$$

la dernière de ces fonctions est constante. On voit, en outre, par les équations (3) :

1°. Que deux fonctions consécutives ne peuvent s'annuler pour une même valeur de z comprise entre -2 et $+2$; car alors toutes les suivantes s'annuleraient pour cette valeur de z, ce qui est impossible, la dernière étant une constante différente de zéro.

2°. Que, si une fonction s'annule pour une valeur de z comprise entre -2 et $+2$, celle qui la précède et celle qui la suit sont de signes contraires pour cette même valeur de z.

Il résulte de là que, si l'on veut appliquer la méthode de M. Sturm à l'équation

$$V_n = 0, \tag{5}$$

on pourra substituer la suite (4) à la suite des fonctions que l'on obtiendrait en exécutant sur V_n et sa dérivée l'opération du plus grand commun diviseur, avec la précaution qu'exige la méthode relativement au changement de signe des restes; pourvu qu'on ne fasse varier z que de -2 à $+2$. Et si α et 6 désignent deux nombres quelconques compris entre -2 et $+2$, tels que $\alpha < 6$, l'équation (5) aura autant de racines comprises entre α et 6 qu'il y aura d'unités dans l'excès du nombre des variations des signes de la suite (4) pour $z = \alpha$, sur le nombre des variations des signes de cette suite pour $z = 6$.

Faisons d'abord $z = -2$, les équations (3) donneront

$$V_n = -2\frac{dV_n}{dz}, \quad \frac{d^{p-2}V_n}{dz^{p-2}} = -2\frac{2p-3}{n^2-(p-2)^2}\frac{d^{p-1}V_n}{dz^{p-1}};$$

et, par conséquent, la suite (4) présente n variations de signes pour $z = -2$.

Faisons ensuite $z = +2$; les équations (3) donneront

$$V_n = 2\frac{dV_n}{dz}, \quad \frac{d^{p-2}V_n}{dz^{p-2}} = 2\frac{2p-3}{n^2-(p-2)^2}\frac{d^{p-1}V}{dz^{p-1}},$$

et, par conséquent, la suite (4) ne présente aucune variation pour $z = 2$.

Donc, enfin, l'équation (5) a ses n racines réelles et comprises entre -2 et $+2$.

QUINZIÈME LEÇON.

Résolution de l'équation générale du troisième degré. — Méthode de Hudde. — Méthode de Lagrange. — Comparaison des deux méthodes précédentes. — Méthode de Tschirnaüs. — Méthode d'Euler.

Résolution de l'équation générale du troisième degré.

Je me propose, dans cette leçon, d'exposer les principales méthodes connues pour la résolution des équations du troisième degré.

Méthode de Hudde.

Des diverses méthodes connues pour la résolution de l'équation générale du troisième degré, la plus simple est, sans contredit, celle de Hudde. C'est aussi celle que nous exposerons la première.

Comme on peut toujours faire disparaître le second terme d'une équation, nous considérerons l'équation

$$(1) \qquad x^3 + px + q = 0$$

débarrassée du terme en x^2. Posons

$$(2) \qquad x = y + z,$$

y étant une nouvelle variable et z une fonction de y, que nous nous réservons de déterminer, de manière que l'équation transformée en y rentre, s'il est possible, dans les classes d'équations que nous savons résoudre. Remplaçons dans l'équation (1) x par sa valeur tirée de (2), on aura

$$(y + z)^3 + p(y + z) + q = 0,$$

ou

(3) $$(y^3 + z^3 + q) + (y + z)(3yz + p) = 0.$$

Si, maintenant, on détermine z par la condition que

$$3yz + p = 0,$$

on a

$$z = -\frac{p}{3y},$$

et l'équation (3) se réduit à

$$y^3 - \frac{p^3}{27y^3} + q = 0,$$

ou

(4) $$y^6 + qy^3 - \frac{p^3}{27} = 0.$$

Cette équation en y peut se résoudre à la manière des équations du second degré, car elle ne contient que les puissances y^3 et y^6. Ensuite, quand y sera connu, on aura x par la formule

(5) $$x = y - \frac{p}{3y}.$$

L'équation du sixième degré (4), à laquelle nous ramenons ainsi l'équation proposée, a été appelée par Lagrange la *réduite* ou *résolvante* de l'équation (1).

Quoique cette résolvante ait six racines, l'équation (5) ne donnera pourtant que trois valeurs de x, comme cela doit être. En effet, la résolvante ne change pas quand on change y en $-\frac{p}{3y}$, en sorte que ses six racines forment trois groupes tels, que le produit des deux racines de chaque groupe est égal à $-\frac{p}{3}$, et il est évident que l'équation (5) donnera la même valeur pour x quand on remplacera y successivement par les deux racines d'un même

groupe. Ceci va résulter, au surplus, de l'expression même des valeurs de x dont nous allons nous occuper.

De l'équation (4), on tire cette valeur de y^3,

$$y^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

ou

$$(6) \qquad y^3 = -\frac{q}{2} \pm \sqrt{R},$$

en faisant, pour abréger,

$$R = \frac{q^2}{4} + \frac{p^3}{27};$$

enfin, l'équation (6) donnera

$$(7) \qquad y = \sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}.$$

Cette expression, à cause des valeurs multiples des radicaux, représente bien les six racines de l'équation (4); mais nous admettrons, dans ce qui va suivre, que $\sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}$ représentera seulement l'une des trois racines cubiques de $-\frac{q}{2} \pm \sqrt{R}$. Ce sera celle que l'on voudra, mais ce sera toujours la même; en sorte que, si α et β désignent les deux racines cubiques imaginaires de l'unité, les six racines de l'équation (4) pourront être représentées par

$$(8) \qquad \sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}, \quad \alpha\sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}, \quad \beta\sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}.$$

Et comme des deux radicaux

$$\sqrt[3]{-\frac{q}{2} + \sqrt{R}}, \quad \sqrt[3]{-\frac{q}{2} - \sqrt{R}},$$

le premier nous représente, par notre convention, celle

des trois racines cubiques de $-\frac{q}{2}+\sqrt{R}$ que nous voudrons, le second également celle des trois racines cubiques de $-\frac{q}{2}-\sqrt{R}$ que nous voudrons, et qu'en outre, leur produit a pour cube $-\frac{p^3}{27}$, nous pouvons choisir les valeurs de ces deux radicaux de manière que leur produit soit égal à $-\frac{p}{3}$; on aura alors

$$(9) \qquad \sqrt[3]{-\frac{q}{2}\mp\sqrt{R}} = \frac{-p}{3\sqrt[3]{-\frac{q}{2}\pm\sqrt{R}}}.$$

Si maintenant on porte, dans l'équation (5), chacune des valeurs (8) de y, on aura, en se servant de l'équation (9) et se rappelant que $\alpha\beta=1$, les valeurs suivantes de x

$$\sqrt[3]{-\frac{q}{2}\pm\sqrt{R}} + \sqrt[3]{-\frac{q}{2}\mp\sqrt{R}},$$

$$\alpha\sqrt[3]{-\frac{q}{2}\pm\sqrt{R}} + \beta\sqrt[3]{-\frac{q}{2}\mp\sqrt{R}},$$

$$\beta\sqrt[3]{-\frac{q}{2}\pm\sqrt{R}} + \alpha\sqrt[3]{-\frac{q}{2}\mp\sqrt{R}},$$

qui se réduisent évidemment à trois distinctes, savoir :

$$\sqrt[3]{-\frac{q}{2}+\sqrt{R}} + \sqrt[3]{-\frac{q}{2}-\sqrt{R}},$$

$$\alpha\sqrt[3]{-\frac{q}{2}+\sqrt{R}} + \beta\sqrt[3]{-\frac{q}{2}-\sqrt{R}},$$

$$\beta\sqrt[3]{-\frac{q}{2}+\sqrt{R}} + \alpha\sqrt[3]{-\frac{q}{2}-\sqrt{R}}.$$

Ces trois racines de l'équation (1) pourront être représentées par la formule unique

$$(10)\qquad x=\sqrt[3]{-\frac{q}{2}+\sqrt{R}}+\sqrt[3]{-\frac{q}{2}-\sqrt{R}},$$

dite formule de Cardan, pourvu qu'alors on laisse aux radicaux cubiques toute leur généralité, mais qu'on n'associe ensemble que les valeurs de ces radicaux qui donnent un produit égal à $-\frac{p}{3}$.

Si, dans la formule (10), on combine chaque valeur du premier radical cubique avec chaque valeur du second, on aura en tout neuf valeurs de x, qui seront les racines des trois équations

$$x^3+px+q=0,$$
$$x^3+p\alpha x+q=0,$$
$$x^3+p\beta x+q=0;$$

ainsi qu'on s'en assure aisément en faisant disparaître les radicaux de l'équation (10).

Tout ce qui précède a lieu, quelles que soient les quantités p et q, réelles ou imaginaires. Nous allons ajouter quelques détails relatifs seulement au cas où ces coefficients sont réels.

Discussion de la formule de Cardan. p et q étant réels, supposons $R>0$, ou

$$4p^3+27q^2>0,$$

les deux radicaux qui entrent dans l'équation (10) auront chacun une de leurs trois valeurs réelles. Désignons par A la valeur réelle du premier, par B celle du second, les trois valeurs du premier radical seront

$$A,\quad A\alpha,\quad A\beta,$$

celles du second seront

$$B,\ B\alpha,\ B6;$$

et comme les valeurs des deux radicaux, qu'il faut prendre ensemble, doivent avoir un produit réel, on aura, pour les racines de l'équation (1),

$$A + B,$$
$$A\alpha + B6,$$
$$A6 + B\alpha.$$

D'ailleurs,

$$\alpha = \frac{-1+\sqrt{-3}}{2}, \qquad 6 = \frac{-1-\sqrt{-3}}{2};$$

les trois racines de l'équation (1) seront donc

$$A + B \quad \text{et} \quad -\frac{A+B}{2} \pm \frac{A-B}{2}\sqrt{-3}.$$

Ainsi, dans ce cas, l'équation (1) a deux racines imaginaires.

Si l'on a $R = 0$, ou

$$4p^3 + 27q^2 = 0,$$

la seule différence avec le cas précédent est que l'on a ici $B = A$; alors l'équation (1) a ses trois racines réelles, mais deux sont égales entre elles.

Supposons, en troisième lieu, $R < 0$, ou

$$4p^3 + 27q^2 < 0,$$

chacun des radicaux qui entrent dans la valeur de x aura ses trois valeurs imaginaires; mais il est facile de voir que l'équation (1) a ses racines réelles et inégales. Soient, en effet,

$$A + B\sqrt{-1}, \quad \alpha(A + B\sqrt{-1}), \quad 6(A + B\sqrt{-1}),$$

les trois racines cubiques de l'expression imaginaire $-\frac{q}{2}+\sqrt{R}$; l'expression imaginaire conjuguée $-\frac{q}{2}-\sqrt{R}$ aura évidemment pour racines cubiques

$$A-B\sqrt{-1},\quad \beta(A-B\sqrt{-1}),\quad \alpha(A-B\sqrt{-1});$$

et comme les valeurs des deux radicaux qui forment la valeur (10) de x doivent avoir un produit réel, on aura les trois valeurs suivantes de x,

$$\begin{gathered}(A+B\sqrt{-1})+(A-B\sqrt{-1}),\\ \alpha(A+B\sqrt{-1})+\beta(A-B\sqrt{-1}),\\ \beta(A+B\sqrt{-1})+\alpha(A-B\sqrt{-1});\end{gathered}$$

ou, en remplaçant α et β par leurs valeurs,

$$2A,\quad -A+B\sqrt{3},\quad -A-B\sqrt{3}.$$

L'équation (1) a donc ses trois racines réelles, comme nous l'avions annoncé, et il est très-facile de montrer qu'elles sont inégales.

En effet, on ne peut avoir d'abord

$$-A+B\sqrt{3}=-A-B\sqrt{3},$$

car il en résulterait $B=0$, et la quantité $-\frac{q}{2}+\sqrt{R}$ serait égale à la quantité réelle A^3, ce qui est contre l'hypothèse. On ne peut avoir non plus

$$2A=-A\pm B\sqrt{3},$$

car il en résulterait $B=\pm A\sqrt{3}$;
par suite,

$$A+B\sqrt{-1}=A(1\pm\sqrt{-3})=-2\alpha A,$$

et

$$-\frac{q}{2}+\sqrt{R}=-8\alpha^3 A^3=-8A^3,$$

ce qui est encore impossible, puisque le second membre est réel.

Le cas que nous avons examiné en dernier lieu est fort remarquable; car, bien qu'alors les trois racines de l'équation du troisième degré soient réelles, la formule de Cardan présente leurs valeurs sous une forme compliquée d'imaginaires : et si, pour faire disparaître ces imaginaires, on cherchait à mettre les radicaux cubiques qui entrent dans la formule de Cardan sous la forme $A+B\sqrt{-1}$, on trouverait que les quantités A et B dépendent d'une équation toute semblable à la proposée. L'équation en A, par exemple, aurait ses trois racines réelles, et l'on trouverait, par conséquent, une expression de A également compliquée d'imaginaires. C'est pour cette raison que le cas dont il s'agit ici a été nommé le *cas irréductible*.

La formule de Cardan ne peut donc servir à la résolution *numérique* de l'équation du troisième degré que si une seule racine est réelle. Mais dans le cas irréductible, l'équation se résout très-simplement en faisant usage des lignes trigonométriques. Si l'on pose, en effet,

$$\frac{q^2}{4}+\frac{p^3}{27}=-\rho^2\sin^2\omega, \quad -\frac{q}{2}=\rho\cos\omega,$$

la quantité ρ et l'angle ω se trouveront déterminés par les formules

$$\rho=\sqrt{\frac{-p^3}{27}}, \quad \cos\omega=\frac{\frac{-q}{2}}{\sqrt{\frac{-p^3}{27}}},$$

et la formule de Cardan donnera

$$x = \sqrt[3]{\rho}\left(\sqrt[3]{\cos\omega + \sqrt{-1}\sin\omega} + \sqrt[3]{\cos\omega - \sqrt{-1}\sin\omega}\right),$$

$\sqrt[3]{\rho}$ désignant une quantité réelle. On a d'ailleurs

$$\sqrt[3]{\cos\omega + \sqrt{-1}\sin\omega} = \cos\frac{\omega + 2k\pi}{3} + \sqrt{-1}\sin\frac{\omega + 2k\pi}{3},$$

$$\sqrt[3]{\cos\omega - \sqrt{-1}\sin\omega} = \cos\frac{\omega + 2k\pi}{3} - \sqrt{-1}\sin\frac{\omega + 2k\pi}{3},$$

où k a l'une des trois valeurs $0, 1, 2$. On doit donner à k la même valeur dans ces deux formules, car il faut que le produit de leurs premiers membres soit réel; on aura donc

$$x = 2\sqrt[3]{\rho}\cos\frac{\omega + 2k\pi}{3},$$

et les trois racines de l'équation seront

$$2\sqrt[3]{\rho}\cos\frac{\omega}{3},\quad 2\sqrt[3]{\rho}\cos\frac{\omega + 2\pi}{3},\quad 2\sqrt[3]{\rho}\cos\frac{\omega + 4\pi}{3}.$$

On pourra, dans chaque cas, calculer par logarithmes les trois racines dont nous venons de donner l'expression.

Méthode de Lagrange.

Considérons l'équation complète du troisième degré

$$(1) \qquad x^3 + Px^2 + Qx + R = 0,$$

et désignons par x_1, x_2, x_3 ses trois racines. D'après la théorie exposée dans les onzième et douzième leçons, on pourra déterminer les valeurs des racines x_1, x_2, x_3, si l'on parvient à connaître la valeur d'une fonction quelconque de ces racines, tellement choisie cependant, que les six valeurs qu'elle peut prendre par les $1.2.3$ permutations des lettres x_1, x_2, x_3 soient différentes. La mé-

thode de Lagrange, que nous allons exposer ici, consiste à déterminer directement la valeur d'une fonction linéaire des trois racines, telle que

$$t = x_1 + Ax_2 + Bx_3, \tag{2}$$

où A et B désignent des constantes quelconques, et à déduire ensuite de cette fonction l'expression des racines elles-mêmes.

Si l'on fait subir aux lettres x_1, x_2, x_3 toutes les permutations possibles, on aura les six valeurs suivantes de la fonction t :

$$(3)\quad \begin{cases} t_1 = x_1 + Ax_2 + Bx_3, \\ t_2 = x_1 + Ax_3 + Bx_2, \\ t_3 = x_2 + Ax_3 + Bx_1, \\ t_4 = x_2 + Ax_1 + Bx_3, \\ t_5 = x_3 + Ax_1 + Bx_2, \\ t_6 = x_3 + Ax_2 + Bx_1, \end{cases}$$

et cette fonction t dépendra de l'équation du sixième degré

$$(t - t_1)(t - t_2)(t - t_3)(t - t_4)(t - t_5)(t - t_6) = 0, \tag{4}$$

qui pourra être résolue à la manière des équations du second degré, si l'on peut disposer des constantes indéterminées A et B, de façon qu'elle ne renferme que la sixième et la troisième puissance de t. Il faut et il suffit, pour qu'il en soit ainsi, que, t désignant l'une quelconque des racines de l'équation (4), α une racine cubique imaginaire de l'unité, αt et $\alpha^2 t$ soient aussi racines de l'équation (4). Voyons si cette condition peut être remplie. D'abord αt_1 et $\alpha^2 t_1$ ne peuvent être égaux ni à t_2, ni à t_4, ni à t_6, car autrement on aurait $\alpha = 1$; il faut donc que l'on ait

$$\alpha t_1 = t_3, \quad \text{et} \quad \alpha^2 t_1 = t_5,$$

ou

$$\alpha t_1 = t_5; \quad \text{et} \quad \alpha^2 t_1 = t_3.$$

Ces deux dernières équations équivalent aux précédentes, puisque rien ne distingue les racines α et α^2 l'une de l'autre; nous adopterons les dernières, et comme elles doivent avoir lieu, quelles que soient x_1; x_2, x_3, nous en déduirons les valeurs suivantes de A et B,

$$A = \alpha, \quad B = \alpha^2.$$

Il arrive alors que A et B ayant ces valeurs, on a aussi

$$\alpha t_2 = t_4, \quad \alpha^2 t_2 = t_6,$$

en sorte que si l'on prend pour valeur de t

$$t = x_1 + \alpha x_2 + \alpha^2 x_3,$$

l'équation en t aura pour racines

$$t_1, \alpha t_1, \alpha^2 t_1, t_2, \alpha t_2, \alpha^2 t_2,$$

et sera, par conséquent,

$$(t^3 - t_1^3)(t^3 - t_2^3) = 0,$$

ou

(5) $$t^6 - (t_1^3 + t_2^3) t^3 + t_1^3 t_2^3 = 0,$$

en faisant

(6) $$\begin{cases} t_1 = x_1 + \alpha x_2 + \alpha^2 x_3, \\ t_2 = x_1 + \alpha^2 x_2 + \alpha x_3. \end{cases}$$

Lorsque les valeurs de t_1 et t_2 seront connues, celles de x_1, x_2, x_3 le seront aisément; on a, en effet,

(7) $$-P = x_1 + x_2 + x_3,$$

et en ajoutant les équations (6) et (7), il vient, à cause de $\alpha^2 + \alpha + 1 = 0$,

(8) $$x_1 = \frac{-P + t_1 + t_2}{3}.$$

Pour avoir x_2, il faut ajouter les trois équations (6) et (7), après les avoir multipliées respectivement par α^2, α et 1; on a ainsi

(9) $$x_2 = \frac{-P + \alpha^2 t_1 + \alpha t_2}{3},$$

et enfin on obtient la valeur suivante de x_3,

(10) $$x_3 = \frac{-P + \alpha t_1 + \alpha^2 t_2}{3},$$

en ajoutant les équations (6) et (7), après les avoir respectivement multipliées par α, α^2 et 1.

Tout est donc ramené à résoudre l'équation (5), qui est alors une *réduite* ou une *résolvante* de l'équation proposée. Cherchons d'abord à exprimer les coefficients de la résolvante par ceux de l'équation proposée, ce qui est possible, puisque ces coefficients $t_1^3 + t_2^3$ et $t_1^3 t_2^3$ sont des fonctions symétriques des racines de l'équation proposée.

Si l'on multiplie les deux équations (6), et qu'on ait égard à la relation $\alpha^2 + \alpha + 1 = 0$, il vient

$$t_1 t_2 = x_1^2 + x_2^2 + x_3^2 - x_1x_2 - x_1x_3 - x_2x_3,$$
$$= (x_1 + x_2 + x_3)^2 - 3(x_1x_2 + x_1x_3 + x_2x_3);$$

et, par conséquent,

(11) $$t_1 t_2 = P^2 - 3Q;$$

si, enfin, on ajoute les deux équations (6), après les avoir élevées au cube, on a

$$t_1^3 + t_2^3 = 2(x_1^3 + x_2^3 + x_3^3)$$
$$- 3(x_1^2 x_2 + x_2^2 x_1 + x_1^2 x_3 + x_3^2 x_1 + x_2^2 x_3 + x_3^2 x_2) + 12 x_1 x_2 x_3$$
$$= 3(x_1^3 + x_2^3 + x_3^3) - (x_1 + x_2 + x_3)^3 + 18 x_1 x_2 x_3$$
$$= -2P^3 + 9PQ - 27R,$$

la résolvante (5) devient donc

$$t^6 - (-2P^3 + 9PQ - 27R)t^3 + (P^2 - 3Q)^3 = 0.$$

En posant

$$t^3 = \theta,$$

elle se réduit à l'équation du second degré

$$\theta^2 - (-2P^3 + 9PQ - 27R)\theta + (P^2 - 3Q)^3 = 0;$$

et, en appelant θ_1 et θ_2 les deux racines de cette équation, on devra faire

$$t_1 = \sqrt[3]{\theta_1}, \quad t_2 = \sqrt[3]{\theta_2},$$

les équations (8), (9) et (10) deviendront alors

$$x_1 = \frac{-P + \sqrt[3]{\theta_1} + \sqrt[3]{\theta_2}}{3},$$

$$x_2 = \frac{-P + \alpha^2\sqrt[3]{\theta_1} + \alpha\sqrt[3]{\theta_2}}{3},$$

$$x_3 = \frac{-P + \alpha\sqrt[3]{\theta_1} + \alpha^2\sqrt[3]{\theta_2}}{3};$$

on prendra pour $\sqrt[3]{\theta_1}$ l'une quelconque des trois valeurs de ce radical, mais la même dans les trois formules : quant à l'autre radical $\sqrt[3]{\theta_2}$, sa valeur est déterminée quand on a fixé celle de $\sqrt[3]{\theta_1}$, car l'équation (11) nous donne

$$\sqrt[3]{\theta_1} . \sqrt[3]{\theta_2} = P^2 - 3Q.$$

Il suit de là que les trois racines pourront être représentées par la formule unique

$$x = \frac{-P + \sqrt[3]{\theta_1} + \sqrt[3]{\theta_2}}{3},$$

qui a trois valeurs et pas davantage, si l'on considère que $\sqrt[3]{\theta_2}$ y est mis, pour abréger, à la place de $\frac{P^2 - 3Q}{\sqrt[3]{\theta_1}}$.

Comparaison des deux méthodes précédentes.

La méthode de Lagrange, que nous venons d'exposer, est moins simple que celle de Hudde; mais elle est plus directe. Toutefois ces deux méthodes fournissent la même résolvante, et nous allons voir qu'on est naturellement conduit à la méthode de Lagrange, en étudiant à fond celle de Hudde.

Reprenons l'équation générale du troisième degré

$$(1) \qquad x^3 + Px^2 + Qx + R = 0.$$

Pour appliquer la méthode de Hudde, on commence par faire disparaître le second terme, en posant

$$x = -\frac{P}{3} + x',$$

ce qui ramène l'équation à la forme

$$(2) \qquad x'^3 + px' + q = 0;$$

on pose ensuite

$$x' = y - \frac{p}{3y},$$

et l'on obtient enfin cette résolvante

$$(3) \qquad y^6 + qy^3 - \frac{p^3}{27} = 0.$$

Cela posé, si y_1 désigne l'une des trois racines cubiques de $-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$, y_2 celle des trois racines

cubiques de $-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$, qui, multipliée par y_1, donne pour produit $\frac{-p}{3}$, les six racines de l'équation (3) sont

$$y_1, \ \alpha y_1, \ \alpha^2 y_1, \quad y_2, \ \alpha y_2, \ \alpha^2 y_2,$$

et celles de l'équation (2)

$$y_1+y_2, \quad \alpha y_1+\alpha^2 y_2, \quad \alpha^2 y_1+\alpha y_2;$$

par suite, en appelant x_1, x_2, x_3 les trois racines de l'équation (1), on a

$$x_1=-\frac{P}{3}+y_1+y_2,$$

$$x_2=-\frac{P}{3}+\alpha^2 y_1+\alpha y_2,$$

$$x_3=-\frac{P}{3}+\alpha y_1+\alpha^2 y_2.$$

Si l'on ajoute ces équations, après les avoir respectivement multipliées d'abord par 1, α, α^2, puis ensuite par 1, α^2, α, il vient

$$y_1=\frac{x_1+\alpha x_2+\alpha^2 x_3}{3},$$

$$y_2=\frac{x_1+\alpha^2 x_2+\alpha x_3}{3}.$$

On voit par là que la méthode de Hudde revient, au fond, à former une résolvante en y dont la racine ait pour valeur

$$y=\frac{x_1+\alpha x_2+\alpha^2 x_3}{3},$$

et que cette résolvante ne diffère de celle de Lagrange que par le facteur 3 qui divise les racines.

Méthode de Tschirnaüs.

Nous avons déjà eu l'occasion de mentionner la méthode générale de Tschirnaüs, pour faire disparaître d'une équation autant de termes que l'on veut. Il en résulte une méthode pour la résolution des équations du troisième degré, ainsi que nous en avons déjà fait la remarque. Les calculs qu'exige l'application de cette méthode sont plus simples, si l'on a la précaution de débarrasser d'abord l'équation proposée de son second terme.

Soit l'équation

$$(1) \qquad x^3 + px + q = 0,$$

et posons, conformément à la méthode de Tschirnaüs,

$$(2) \qquad y = a + bx + x^2.$$

Si l'on élimine x entre les équations (1) et (2), on obtiendra cette équation en y,

$$(3) \qquad y^3 + Ay^2 + By + C = 0,$$

où l'on fait, pour abréger,

$$A = -3a + 2p,$$
$$B = 3a^2 - 4pa + pb^2 + 3qb + p^2,$$
$$C = -a^3 + 2pa^2 - p^2a + pb^2a - 3qba + qb^3 + pqb - q^2.$$

Quant à la valeur de x en fonction de y, on peut la tirer de l'équation du premier degré en x, que l'on rencontre nécessairement dans le calcul de l'élimination de x entre les équations (1) et (2) ; on trouve ainsi

$$(4) \qquad x = \frac{by - (ab + q)}{y - (a - b^2 - p)}.$$

Enfin, on déterminera a et b de manière que l'on ait

$$A = 0, \quad B = 0.$$

Comme ces équations sont, l'une du second degré, l'autre du premier entre a et b, on trouvera facilement les valeurs de a et b ; l'équation (3) donnera alors

$$y = \sqrt[3]{-C},$$

et l'équation (4) fera connaître les trois valeurs de x.

Cette méthode, fort simple au point de vue théorique, conduit à des calculs très-laborieux.

Méthode d'Euler.

Nous nous bornerons à mentionner cette méthode, qui rentre, au fond, dans celle de Tschirnaüs. Elle consiste à éliminer y entre deux équations de la forme

$$ay^2 + by + c = x, \quad y^3 = d,$$

et à identifier l'équation finale en x avec l'équation proposée, dont la résolution s'ensuivra évidemment. On peut disposer, à volonté, de la valeur de l'une des indéterminées a, b, c, d; on peut faire, par exemple, $a = 1$ ou $d = 1$.

SEIZIÈME LEÇON.

Des équations du troisième degré dont deux racines peuvent s'exprimer rationnellement en fonction de la troisième et des quantités connues. — Étude d'une classe étendue d'équations numériques du troisième degré, qui possèdent une propriété remarquable.

Des équations du troisième degré dont deux racines peuvent s'exprimer rationnellement en fonction de la troisième et des quantités connues.

Considérons l'équation du troisième degré débarrassée du second terme

$$(1) \qquad x^3 + px + q = 0,$$

et dans laquelle p et q désignent des fonctions rationnelles de quantités quelconques qu'on regarde comme connues. On peut, comme on va voir, exprimer, dans un cas assez étendu, deux quelconques des trois racines de l'équation (1) en fonction rationnelle de la troisième et des quantités connues.

Désignons par y et z deux quantités ayant pour produit $-\frac{p}{3}$, et dont les cubes ont respectivement pour valeurs

$$(2) \qquad \begin{cases} y^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \\ z^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} : \end{cases}$$

soient aussi α et β les deux racines cubiques imaginaires de l'unité : les trois racines x, x_1, x_2 de l'équation (1)

ont pour valeurs

$$(3)\qquad \begin{cases} x = y + z, \\ x_1 = \alpha y + 6 z, \\ x_2 = 6 y + \alpha z, \end{cases}$$

ainsi qu'on l'a vu dans la dernière leçon; on a d'ailleurs

$$\alpha = \frac{-1+\sqrt{-3}}{2}, \qquad 6 = \frac{-1-\sqrt{-3}}{2};$$

par suite, les valeurs de x_1 et x_2 deviennent

$$(4)\qquad \begin{cases} x_1 = -\frac{y+z}{2} + \frac{y-z}{2}\sqrt{-3}, \\ x_2 = -\frac{y+z}{2} - \frac{y-z}{2}\sqrt{-3}, \end{cases}$$

ou, à cause de la première des équations (3),

$$(5)\qquad \begin{cases} x_1 = -\frac{x}{2} + \frac{y-z}{2}\sqrt{-3}, \\ x_2 = -\frac{x}{2} - \frac{y-z}{2}\sqrt{-3}. \end{cases}$$

On voit, par là, que x_1 et x_2 sont exprimables en fonction rationnelle de x et des quantités connues, si la différence $y-z$ l'est elle-même.

On a, par les équations (2),

$$y^3 + z^3 = -q, \qquad y^3 - z^3 = \sqrt{q^2 + \frac{4p^3}{27}},$$

et, par hypothèse,

$$yz = -\frac{p}{3};$$

d'ailleurs

$$y - z = \frac{y^3 - z^3}{y^2 + yz + z^2} = \frac{y^3 - z^3}{(y+z)^2 - yz},$$

donc

$$y - z = \frac{\sqrt{q^2 + \frac{4p^3}{27}}}{x^2 + \frac{p}{3}};$$

portant cette valeur de $y-z$ dans les équations (5), il vient

$$x_1 = -\frac{x}{2} + \frac{\sqrt{-4p^3 - 27q^2}}{2(3x^2 + p)},$$

$$x_2 = -\frac{x}{2} - \frac{\sqrt{-4p^3 - 27q^2}}{2(3x^2 + p)};$$

d'où il résulte que x_1 et x_2 s'exprimeront en fonction rationnelle de x et des quantités connues, si $\sqrt{-4p^3 - 27q^2}$ est lui-même exprimable en fonction rationnelle des quantités connues dont p et q dépendent.

On peut simplifier les précédentes expressions de x_1 et x_2. Nous ferons d'abord

(6) $$4p^3 + 27q^2 = -r^2,$$

r pouvant être réel ou imaginaire; et remarquant ensuite que x doit satisfaire à l'équation (1), nous remplacerons dans les valeurs de x_1 et x_2, x^2 par $-\frac{px+q}{x}$, on aura ainsi

$$x_1 = -\frac{x}{2} - \frac{rx}{2(3q + 2px)},$$

$$x_2 = -\frac{x}{2} + \frac{rx}{2(3q + 2px)}.$$

Comme ces deux formules se déduisent l'une de l'autre par le changement de r en $-r$, les valeurs de x_1 et x_2

seront toutes deux comprises dans la formule unique

$$(7)\quad \left\{\begin{aligned} X &= -\frac{x}{2} + \frac{rx}{2(3q+2px)}, \\ &= \frac{-2px^2 + (r-3q)x}{2(3q+2px)}, \end{aligned}\right.$$

où l'on remplacera r successivement par ses deux valeurs tirées de l'équation (6).

X est une fonction rationnelle non entière d'une racine x de l'équation (1); on pourra donc, par l'un des procédés indiqués dans la deuxième leçon, mettre sa valeur sous la forme d'un polynôme du second degré en x.

Pour cela, on divisera d'abord le premier membre de l'équation (1) par $3q + 2px$, et l'on sera conduit ainsi à l'égalité suivante :

$$\begin{aligned} 8p^3(x^3+px+q) = (2px+3q)(4p^2x^2 - 6pqx + 4p^3 + 9q^2) \\ - q(4p^3 + 27q^2) = 0, \end{aligned}$$

d'où l'on tire

$$3q + 2px = \frac{-qr^2}{4p^2x^2 - 6pqx + 4p^3 + 9q^2},$$

et la valeur de X, donnée par l'équation (7), sera alors

$$\begin{aligned} X &= \frac{-1}{2qr^2}[-2px^2 + (r-3q)x][4p^2x^2 - 6pqx + 4p^3 + 9q^2], \\ &= \frac{1}{2qr^2}\left[\begin{aligned} 8p^3x^4 - 4p^2rx^3 + (8p^4 + 6pqr)x^2 \\ -(4p^3+9q^2)(r-3q)x \end{aligned}\right]; \end{aligned}$$

enfin on chassera de cette expression de X, x^3 et x^4, à l'aide des équations

$$x^3 = -px - q, \qquad x^4 = -px^2 - qx,$$

et l'on aura

$$(8)\qquad X = \frac{1}{2r}[6px^2 - (9q + r)x + 4p^2].$$

Telle est là formule la plus simple par laquelle on puisse exprimer deux racines de l'équation (1) en fonction rationnelle de la troisième et des quantités connues, lorsque r est une quantité rationnelle.

Mais on peut aussi, comme nous l'avons remarqué dans la deuxième leçon, mettre cette valeur de X sous forme d'une fraction ayant pour numérateur et pour dénominateur un binôme du premier degré en x.

Pour cela, on divisera le premier membre de l'équation (1) par $6px^2-(9q+r)x+4p^2$, après l'avoir préalablement multiplié par $36p^2$ pour éviter les dénominateurs; on trouvera pour quotient

$$6px+(9q+r),$$

et pour reste

$$2r(9q-r)x-4p^2r,$$

en ayant égard à l'équation (6). On aura donc

$$\begin{aligned}&36p^2(x^3+px+q)\\&=[6px^2-(9q+r)x+4p^2][6px+(9q+r)]\\&+[2r(9q-r)x-4p^2r]=0,\end{aligned}$$

et par conséquent

$$6px^2-(9q+r)x+4p^2=\frac{-2r(9q-r)x+4p^2r}{6px+(9q+r)};$$

la valeur de X sera donc

$$(9)\qquad X=\frac{-(9q-r)x+2p^2}{6px+(9q+r)}.$$

Si p et q désignent des quantités numériques déterminées, et que la quantité $4p^3+27q^2=-r^2$ soit négative, ce qui est la condition nécessaire pour que l'équation (1) ait ses trois racines réelles, les deux valeurs de r seront réelles et de signes contraires; en désignant donc spécialement par r celle de ces deux valeurs qui est posi-

tive, on aura les expressions suivantes des deux racines x_1 et x_2 en fonction de la troisième x

$$(10)\quad x_1 = \frac{-(9q-r)x+2p^2}{6px+(9q+r)}, \quad x_2 = \frac{-(9q+r)x+2p^2}{6px+(9q-r)}.$$

Nous allons faire, dans ce qui va suivre, une application assez importante de ces formules.

Étude d'une classe étendue d'équations numériques du troisième degré, qui possèdent une propriété remarquable.

Si l'on développe en fraction continue, conformément à la méthode de Lagrange, les trois racines x, x_1, x_2 de l'équation

$$x^3 - 7x + 7 = 0,$$

on trouve

$$-x = 3 + \frac{1}{y}, \qquad x_1 = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{y}}}},$$

$$x_2 = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{y}}}},$$

y désignant la racine plus grande que 1 de l'équation

$$y^3 - 20y^2 - 9y + 1 = 0,$$

en sorte que les trois fractions continues, dans lesquelles se développent les racines x, x_1, x_2, se terminent par les mêmes quotients.

Cette propriété curieuse de l'équation que nous venons

de considérer a été remarquée depuis longtemps, mais c'est tout récemment que M. Lobatto s'est proposé, le premier, de trouver quelles sont les équations du troisième degré, à coefficients commensurables, qui possèdent cette propriété. Ce géomètre a complétement résolu la question, pour les équations de la forme

$$x^3 + px + q = 0,$$

dans un Mémoire qu'il a publié dans le tome IX du *Journal des Mathématiques pures et appliquées* de M. Liouville. Nous suivrons à peu près la marche qu'il a indiquée.

Si une équation du troisième degré, débarrassée du second terme, a ses trois racines réelles, le coefficient de la première puissance de x est négatif; nous considérerons donc l'équation

$$x^3 - px + q = 0, \tag{1}$$

et nous supposerons p et q positifs et commensurables (le cas de q négatif se ramènerait à celui de q positif par le simple changement de x en $-x$), en sorte que l'équation (1) aura une racine négative et deux racines positives. Nous désignerons par $-x$ la racine négative, par x_1 et x_2 les deux racines positives, et en faisant

$$r = +\sqrt{4p^3 - 27q^2}, \tag{2}$$

on déduira des formules précédemment établies, par de simples changements de signes,

$$x_1 = \frac{(9q - r)x + 2p^2}{6px + (9q + r)}, \quad x_2 = \frac{(9q + r)x + 2p^2}{6px + (9q - r)}. \tag{3}$$

Supposons maintenant que les fractions continues qui représentent x et x_1 soient terminées par un même quotient complet y; d'après les propriétés des fractions

continues, on aura, pour x et x_1, des valeurs de la forme suivante :

$$(4) \qquad x = \frac{Ny + M}{N'y + M'}, \quad x_1 = \frac{Qy + P}{Q'y + P'},$$

M, N, etc., étant des nombres entiers positifs assujettis à vérifier les équations

$$(5) \qquad NM' - MN' = \pm 1, \quad QP' - PQ' = \pm 1.$$

De la première des équations (4), on tire

$$y = \frac{M - M'x}{N'x - N},$$

et, en portant cette valeur de y dans la seconde, il vient

$$(6) \qquad x_1 = \frac{Ax + B}{A'x + B'},$$

en faisant, pour abréger,

$$A = PN' - QM', \quad B = QM - PN,$$
$$A' = P'N' - Q'M', \quad B' = Q'M - P'N;$$

d'où l'on déduit aisément

$$(7) \qquad AB' - BA' = (NM' - MN')(QP' - PQ') = \pm 1.$$

Les valeurs de x_1, données par les équations (3) et (6), doivent être identiques; car, s'il en est autrement, en égalant ces deux valeurs de x_1, on aura une équation du second ou du premier degré à coefficients commensurables, ou du moins qui ne contiendront que le radical r: cette équation, après qu'on y aura changé x en $-x$, aura, avec la proposée (1), une ou deux racines communes, et, dans l'un et l'autre cas, le premier membre de l'équation (1) admettra un diviseur linéaire commensurable ou ne contenant que le radical r. Si ce diviseur linéaire est commensurable, l'équation proposée (1) aura une racine

commensurable. Si ce diviseur contient le radical r, et que r soit incommensurable, l'équation proposée (1) aura une racine de la forme $\alpha + 6r$, elle admettra donc aussi $\alpha - 6r$ pour racine, et la troisième racine sera alors commensurable; d'où il suit que si l'équation (1) n'a pas de racine commensurable, comme nous le supposons évidemment dans cette recherche, les deux valeurs de x_1, données par les équations (3) et (6), sont nécessairement identiques: on a donc

$$(8) \qquad \frac{9q - r}{A} = \frac{2p^2}{B} = \frac{6p}{A'} = \frac{9q + r}{B'} = \lambda.$$

On peut déterminer aisément la valeur λ commune à chacun de ces rapports. On tire, en effet, de ces équations (8)

$$\lambda^2(AB' - BA') = -4r^2;$$

et comme $AB' - BA'$ doit être égal à ± 1, il faut qu'ici

$$AB' - BA' = -1, \quad \text{et} \quad \lambda^2 = 4r^2,$$

d'où

$$\lambda = \pm 2r,$$

et même $\lambda = 2r$, à cause que les fractions (8) sont évidemment positives: les équations (8) donneront alors

$$\frac{9q - r}{2r} = A, \quad \frac{2p^2}{2r} = B, \quad \frac{6p}{2r} = A', \quad \frac{9q + r}{2r} = B'.$$

Donc, pour que les deux racines $-x$ et x_1 de l'équation (1) se terminent par les mêmes quotients incomplets, il faut que

$$(9) \qquad \frac{9q - r}{2r}, \quad \frac{2p^2}{2r}, \quad \frac{6p}{2r}, \quad \frac{9q + r}{2r},$$

soient des nombres entiers; ce qui exige, en particulier, que r soit commensurable, puisque p et q le sont par hypothèse.

On serait arrivé exactement à la même condition si, au lieu de considérer les racines $-x$ et x_1, on eût pris $-x$ et x_2.

Je dis maintenant que les conditions que nous venons de trouver sont suffisantes, et que, si les quantités (9) sont des nombres entiers, les trois racines de l'équation (1) étant développées en fraction continue, se termineront toutes trois par un même quotient complet.

Posons

$$(10) \quad \frac{9q-r}{2r} = \text{A}, \quad \frac{2p^2}{2r} = \text{B}, \quad \frac{6p}{2r} = \text{A}', \quad \frac{9q+r}{2r} = \text{B}',$$

les formules (3) deviendront

$$(11) \qquad x_1 = \frac{\text{A}x + \text{B}}{\text{A}'x + \text{B}'}, \qquad x_2 = \frac{\text{B}'x + \text{B}}{\text{A}'x + \text{A}};$$

les équations (10) donnent d'ailleurs

$$(12) \qquad \text{AB}' - \text{BA}' = -1,$$

et par hypothèse, A, B, A′, B′ sont des nombres entiers.

Cela posé, pour établir la proposition que nous avons en vue, nous commencerons par démontrer le lemme suivant.

Lemme. — *Si* A, B, A′, B′ *sont quatre nombres entiers tels, que* $\text{A} > \text{B}$, $\text{A}' > \text{B}'$, *et qui satisfont à la condition*

$$\text{AB}' - \text{BA}' = \pm 1,$$

on pourra toujours considérer les fractions $\frac{\text{B}}{\text{B}'}$ *et* $\frac{\text{A}}{\text{A}'}$ *comme deux réduites consécutives d'une même fraction continue.*

Réduisons, en effet, $\frac{\text{A}}{\text{A}'}$ en fraction continue, et arrangeons-nous de manière que le nombre des quotients soit pair ou impair, suivant que $\text{AB}' - \text{BA}'$ est égal à $+1$ ou à -1. Cela est toujours possible; car on peut, si on le

juge à propos, diminuer d'une unité le dernier quotient obtenu, et prendre un quotient de plus égal à 1. Formons les réduites de cette fraction continue, et désignons par $\frac{M}{M'}$ l'avant-dernière, c'est-à-dire celle qui précède $\frac{A}{A'}$, on aura

$$AM' - MA' = \pm 1 = AB' - BA',$$

et, par conséquent,

$$A(M' - B') = A'(M - B).$$

Or je dis que cette dernière égalité exige que l'on ait $M = B$, $M' = B'$; car si cela n'avait pas lieu, A, qui divise le premier membre de l'équation précédente, diviserait aussi le second, et comme il est évidemment premier avec A', il diviserait $M - B$, ce qui est impossible, puisque M et B sont tous deux moindres que A.

Il suit de là que l'on peut supposer que $\frac{B}{B'}$ est l'avant-dernière réduite de la fraction continue dans laquelle se développe $\frac{A}{A'}$. Notre lemme est donc démontré.

Revenons maintenant au théorème qu'il s'agit d'établir (*).

Si l'on a à la fois

$$A > B, \quad A' > B', \quad x > 1,$$

il est évident, d'après la première équation (11), que x sera un quotient complet de la fraction continue dans laquelle se développe x_1; car, à cause de l'équation (12), si l'on fait le développement de $\frac{A}{A'}$ en fraction continue, on

(*) Le Mémoire de M. Lobatto renferme quelques inexactitudes, qui pourtant n'infirment en rien les conclusions de l'auteur.

aura, par exemple,

$$\frac{A}{A'} = \alpha + \frac{1}{6 + \ldots + \frac{1}{\gamma + \frac{1}{\delta}}}, \qquad \frac{B}{B'} = \alpha + \frac{1}{6 + \ldots + \frac{1}{\gamma}},$$

et, d'après les propriétés des fractions continues,

$$x_1 = \alpha + \frac{1}{6 + \ldots + \frac{1}{\gamma + \frac{1}{\delta + \frac{1}{x}}}}.$$

Supposons que l'on n'ait pas à la fois $A > B$, $A' > B'$, mais que x soit > 1, et posons

$$x = a + \frac{1}{z},$$

a étant le plus grand entier contenu dans x, la valeur de x_1 devient

$$x_1 = \frac{(Aa + B)z + A}{(A'a + B')z + A'} = \frac{Cz + A}{C'z + A'};$$

ici l'on a évidemment, a n'étant pas nul,

$$C > A, \quad C' > A'$$

et

$$CA' - AC' = +1, \quad \text{à cause de} \quad AB' - BA' = -1;$$

d'où il résulte, évidemment, que z sera un quotient complet de la fraction continue dans laquelle x_1 se développe. Cette conclusion est en défaut si a est nul; car alors la valeur x_1 est

$$x_1 = \frac{Bz + A}{B'z + A'},$$

et il se peut qu'on n'ait pas à la fois $B > A$ et $B' > A'$. Posons alors

$$z = b + \frac{1}{u},$$

b étant l'entier le plus grand contenu dans z; on aura

$$x_1 = \frac{(Bb + A)u + B}{(B'b + A')u + B'} = \frac{Du + B}{D'u + B'}.$$

Comme b ne peut être nul, on a évidemment $D > B$, $D' > B'$; d'ailleurs $DB' - BD' = -1$, donc u sera un quotient complet de x_1.

Il résulte de ce qui précède que l'un des trois premiers quotients complets de la racine négative $-x$ sera nécessairement un quotient complet de la racine positive x_1, et par conséquent aussi de la racine x_2; car tous nos raisonnements s'appliquent à x_2 qui se déduit de x_1, en changeant A et B' l'un dans l'autre.

Formation des équations qui possèdent la propriété précédente. — Nous allons former les équations qui possèdent la propriété que nous venons d'étudier.

Il s'agit des équations de la forme

$$x^3 - px + q = 0,$$

et qui sont telles, qu'en posant

$$r^2 = 4p^3 - 27q^2$$

on ait

$$(1) \qquad 9q - r = 2rA,$$

$$(2) \qquad p^2 = rB,$$

$$(3) \qquad 3p = rA',$$

$$(4) \qquad (9q + r) = 2rB',$$

A, B, A', B' étant des nombres entiers; et il en résulte

$$(5) \qquad AB' - BA' = -1$$

L'équation (5) étant une conséquence des quatre premières, nous pouvons nous borner aux équations (1), (3), (4), (5), et même substituer aux équations (1) et (4) celles qu'on en déduit par addition et soustraction, savoir :

$$9q = r(A + B'), \quad B' - A = 1.$$

De ces dernières combinées avec les équations (2) et (5), on tire

$$B' = A + 1, \tag{6}$$

$$B = \frac{A^2 + A + 1}{A'}, \tag{7}$$

$$q = \frac{2A + 1}{9} r, \tag{8}$$

$$p = \frac{A'}{3} r. \tag{9}$$

Des équations (8) et (9) combinées avec l'équation $r^2 = 4p^3 - 27q^2$, on tire

$$r = \frac{9(2A + 1)^2 + 27}{4A'^3};$$

par suite, les équations (8) et (9) donnent

$$p = 3\frac{(2A + 1)^2 + 3}{4A'^2} = \frac{3(A^2 + A + 1)}{A'^2},$$

$$q = \frac{(2A + 1)^3 + 3(2A + 1)}{4A'^3} = \frac{2A^3 + 3A^2 + 3A + 1}{A'^3}.$$

Dans ces formules, A peut être considéré comme un nombre entier absolument arbitraire, et A' n'est assujetti qu'à la seule condition de satisfaire à l'équation (7), c'est-à-dire de diviser $A^2 + A + 1$.

Il résulte de là que les équations du troisième degré

dont nous nous occupons ont la forme générale que voici :

$$x^3 - 3\frac{A^2+A+1}{A'^2}x + \frac{2A^3+3A^2+3A+1}{A'^3} = 0,$$

A désignant un nombre entier quelconque, et A' un diviseur quelconque de A^2+A+1. L'équation $x^3-7x+7=0$ se déduit de cette équation générale, en faisant $A=4$; $A'=3$.

M. Lobatto s'est borné, dans son Mémoire, à l'étude des équations du troisième degré débarrassées du second terme. On arriverait à des résultats plus étendus, en considérant les équations complètes; car on comprend qu'une équation complète puisse posséder la propriété que M. Lobatto a étudiée, et ne pas la conserver quand on l'aura débarrassée de son second terme. Cette extension des recherches de M. Lobatto ne présente aucune difficulté, car l'équation la plus générale du troisième degré peut être mise sous la forme

$$(x-a)^3 + p(x-a) + q = 0,$$

et l'on peut aisément exprimer deux racines en fonction rationnelle de la troisième, en se servant des formules que nous avons établies précédemment. Ces formules feront connaître ensuite les conditions pour que les fractions continues dans lesquelles se développent les trois racines puissent se terminer par les mêmes quotients incomplets : il n'y a qu'à employer des raisonnements tout semblables à ceux que nous avons faits; mais je crois devoir me borner, ici, à cette simple indication.

DIX-SEPTIÈME LEÇON.

Résolution de l'équation générale du quatrième degré. — Méthode de Louis Ferrari. — Étude de la résolvante. — Méthode de Lagrange. — Méthode de Descartes. — Méthodes de Tschirnaüs et d'Euler.

Résolution de l'équation générale du quatrième degré.

Nous allons exposer, dans cette leçon, les principales méthodes connues pour la résolution de l'équation générale du quatrième degré.

Méthode de Louis Ferrari.

La méthode la plus simple pour résoudre l'équation du quatrième degré, est aussi la plus ancienne; c'est celle de Louis Ferrari : elle consiste à faire en sorte que les deux membres de l'équation soient des carrés, et elle ramène par suite la résolution de l'équation du quatrième degré à celle de deux équations du second.

Soit l'équation

$$(1) \qquad x^4 + px^3 + qx^2 + rx + s = 0;$$

en ne conservant dans le premier membre que les deux premiers termes, elle devient

$$x^4 + px^3 = -qx^2 - rx - s,$$

et, en ajoutant aux deux membres $\frac{p^2x^2}{4}$, afin que le premier membre devienne un carré,

$$(2) \qquad \left(x^2 + \frac{p}{2}x\right)^2 = \left(\frac{p^2}{4} - q\right)x^2 - rx - s.$$

Mise sous cette forme, l'équation proposée se résoudrait immédiatement, si le second membre était un carré; car il suffirait alors d'extraire la racine carrée des deux membres, et l'équation ne serait plus que du second degré.

C'est à ce cas très-particulier que la méthode de Ferrari ramène tous les autres.

Désignons par y une quantité indéterminée, et ajoutons aux deux membres de l'équation (2) la même quantité

$$\left(x^2 + \frac{p}{2}x\right)y + \frac{y^2}{4},$$

il vient

$$(3)\quad \left(x^2+\frac{p}{2}x+\frac{y}{2}\right)^2 = \left(\frac{p^2}{4}-q+y\right)x^2+\left(\frac{py}{2}-r\right)x+\left(\frac{y^2}{4}-s\right).$$

Maintenant, déterminons y, de manière que le second membre de l'équation (3) soit un carré. Il suffit, pour cela, que l'on ait

$$\left(\frac{py}{2}-r\right)^2 = \left(\frac{p^2}{4}-q+y\right)(y^2-4s),$$

ou

$$(4)\quad y^3 - qy^2 + (pr-4s)y - s(p^2-4q) - r^2 = 0;$$

et si l'on connaît une seule racine de cette équation en y, la résolution de l'équation proposée (1) s'ensuivra immédiatement, car l'équation (3), qui est la même que (1), peut s'écrire comme il suit :

$$\left(x^2+\frac{p}{2}x+\frac{y}{2}\right)^2 - \left(\frac{p^2}{4}-q+y\right)\left[x+\frac{p\frac{y}{2}-r}{2\sqrt{\frac{p^2}{4}-q+y}}\right]^2 = 0,$$

et se décompose dans les deux suivantes, qui sont du second degré,

$$(5)\quad \begin{cases} x^2+\left(\frac{p}{2}+\sqrt{\frac{p^2}{4}-q+y}\right)x+\left[\frac{y}{2}+\frac{\frac{py}{2}-r}{2\sqrt{\frac{p^2}{4}-q+y}}\right]=0, \\ x^2+\left(\frac{p}{2}-\sqrt{\frac{p^2}{4}-q+y}\right)x+\left[\frac{y}{2}-\frac{\frac{py}{2}-r}{2\sqrt{\frac{p^2}{4}-q+y}}\right]=0. \end{cases}$$

L'équation (4), qui est du troisième degré, sera donc ici la *réduite* ou la *résolvante* de l'équation (1). Nous avons vu qu'on peut exprimer par radicaux les racines de l'équation générale du troisième degré, il s'ensuit que l'équation du quatrième degré jouit de la même propriété, car les équations (5) permettent d'exprimer les quatre racines de l'équation (1) en fonction des coefficients et d'une racine quelconque y de la résolvante.

EXEMPLE. — Considérons l'équation

$$x^4 + x^3 - 4x^2 - 4x + 1 = 0,$$

dont les racines ont pour valeurs absolues le côté et les diagonales du polygone régulier de trente côtés inscrit dans le cercle de rayon 1. La résolvante (4) sera ici

$$y^3 + 4y^2 - 8y - 33 = 0,$$

et a -3 pour racine; l'équation proposée se décompose alors dans les deux suivantes :

$$x^2 + \frac{1+\sqrt{5}}{2}x - \left(\frac{-1+\sqrt{5}}{2}\right)^2 = 0,$$

$$x^2 + \frac{-1+\sqrt{5}}{2}x - \left(\frac{1+\sqrt{5}}{2}\right)^2 = 0;$$

et, en général, en appliquant la méthode de Ferrari à une équation du quatrième degré à coefficients commensurables dont les racines ne doivent pas contenir, dans leur expression, de radicaux cubiques, on arrivera toujours à une résolvante qui aura une racine commensurable.

Étude de la résolvante.

Nous venons de voir comment les quatre racines de l'équation proposée peuvent s'exprimer à l'aide d'une seule racine de la résolvante; nous allons étudier à son tour

cette résolvante, et examiner de quelle manière ses racines sont formées avec celles de la proposée.

Désignons toujours par y une racine quelconque de la résolvante, et par x_1, x_2, x_3, x_4 les quatre racines de l'équation proposée, savoir, par x_1 et x_2 celles qui appartiennent à la première des équations (5); par x_3 et x_4 celles qui appartiennent à la seconde. On aura alors

$$x_1 x_2 = \frac{y}{2} + \frac{\frac{py}{2} - r}{2\sqrt{\frac{p^2}{4} - q + y}},$$

$$x_3 x_4 = \frac{y}{2} - \frac{\frac{py}{2} - r}{2\sqrt{\frac{p^2}{4} - q + y}};$$

et, en ajoutant,

$$y = x_1 x_2 + x_3 x_4.$$

La résolvante a donc pour racine la fonction

$$x_1 x_2 + x_3 x_4$$

des quatre racines de la proposée, qui n'a effectivement que trois valeurs, quand on y échange les racines les unes dans les autres de toutes les manières possibles.

Posons

$$t = 2\sqrt{\frac{p^2}{4} - q + y},$$

d'où

$$y = \frac{t^2}{4} - \left(\frac{p^2}{4} - q\right);$$

la résolvante en y se transformera dans une équation en t, qui sera du sixième degré, mais qui ne contiendra que des puissances paires de t. Cette équation ne sera pas plus difficile à résoudre que l'équation (4), et on peut la

prendre pour résolvante à la place de cette dernière. Les équations (5), dans lesquelles se décompose l'équation proposée, deviennent alors

$$x^2 + \left(\frac{p+t}{2}\right)x + \frac{1}{2}\left(\frac{t^2}{4} - \frac{p^2}{4} + q\right) + \frac{\frac{p}{2}\left(\frac{t^2}{4} - \frac{p^2}{4} + q\right) - r}{2t} = 0,$$

$$x^2 + \left(\frac{p-t}{2}\right)x + \frac{1}{2}\left(\frac{t^2}{4} - \frac{p^2}{4} + q\right) - \frac{\frac{p}{2}\left(\frac{t^2}{4} - \frac{p^2}{4} + q\right) - r}{2t} = 0,$$

et l'on en déduira les quatre racines de la proposée, si l'on connaît une seule racine de la résolvante en t.

Les équations précédentes ont pour racines, la première, x_1 et x_2, la seconde, x_3 et x_4; on a donc

$$x_1 + x_2 = \frac{p+t}{2},$$

$$x_3 + x_4 = \frac{p-t}{2},$$

et, en retranchant,

$$t = x_1 + x_2 - x_3 - x_4.$$

Telle est l'expression de la racine de la résolvante en t. C'est une fonction linéaire des racines de la proposée, qui peut prendre effectivement six valeurs égales deux à deux et de signes contraires, par les permutations des racines x_1, x_2, x_3, x_4.

Méthode de Lagrange.

D'après la théorie générale exposée dans les onzième et douzième leçons, on peut exprimer rationnellement les quatre racines de l'équation générale du quatrième degré par une fonction de ces racines telle, que les 1.2.3.4 valeurs qu'on en déduit par les permutations soient différentes. Une pareille fonction dépend d'une équation du vingt-quatrième degré; mais nous venons de voir, par

l'analyse de la méthode de Ferrari, qu'il suffit, pour résoudre l'équation du quatrième degré, de connaître une fonction des racines qui ait trois valeurs seulement, ou six valeurs égales deux à deux et de signes contraires.

La formation à priori de l'équation dont dépend une pareille fonction des racines de la proposée, et la détermination subséquente de ces racines, constitue une nouvelle méthode due à Lagrange, et que nous allons actuellement exposer.

Soit l'équation

$$(1) \qquad x^4 + px^3 + qx^2 + rx + s = 0,$$

et désignons par x_1, x_2, x_3, x_4 ses quatre racines. La fonction la plus simple de ces racines parmi celles qui ne peuvent acquérir que trois valeurs est $x_1x_2 + x_3x_4$; posons donc

$$y = x_1x_2 + x_3x_4,$$

et commençons par chercher la valeur de y, ou plutôt l'équation du troisième degré dont elle dépend.

Soient y_1, y_2, y_3 les trois valeurs que peut acquérir y, on aura

$$y_1 = x_1x_2 + x_3x_4, \quad y_2 = x_1x_3 + x_2x_4, \quad y_3 = x_1x_4 + x_2x_3,$$

et l'équation en y sera

$$(2) \; y^3 - (y_1 + y_2 + y_3)y^2 + (y_1y_2 + y_1y_3 + y_2y_3)y - y_1y_2y_3 = 0.$$

Les coefficients de cette équation (2) sont des fonctions symétriques des racines de l'équation (1), et peuvent, par conséquent, s'exprimer par les coefficients p, q, r, s. On a

$$y_1 + y_2 + y_3 = (x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4) = q,$$

$$y_1y_2 + y_1y_3 + y_2y_3$$
$$= (x_1 + x_2 + x_3 + x_4)(x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4)$$
$$- 4x_1x_2x_3x_4 = pr - 4s,$$

$$y_1y_2y_3 = x_1x_2x_3x_4$$
$$\times [(x_1 + x_2 + x_3 + x_4)^2 - 4(x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4)]$$
$$+ (x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4)^2 = s(p^2 - 4q) + r^2;$$

l'équation résolvante en y est donc

$$(3)\quad y^3 - qy^2 + (pr - 4s)y - [s(p^2 - 4q) + r^2] = 0.$$

Nous savons résoudre cette équation, qui est du troisième degré; voyons maintenant comment on obtiendra les valeurs des racines x_1, x_2, x_3, x_4.

Soit y_1 une racine quelconque de l'équation (3), on aura

$$x_1 x_2 + x_3 x_4 = y_1;$$

d'ailleurs

$$x_1 x_2 \times x_3 x_4 = s;$$

donc $x_1 x_2$ et $x_3 x_4$ sont les racines de l'équation du second degré

$$(4)\quad z^2 - y_1 z + s = 0.$$

Soient z_1 et z_2 les racines de cette équation (4), on aura

$$x_1 x_2 = z_1, \quad x_3 x_4 = z_2;$$

connaissant ainsi les fonctions $x_1 x_2$ et $x_3 x_4$, on voit de suite qu'on doit en déduire rationnellement les sommes $x_1 + x_2$ et $x_3 + x_4$, qui sont des fonctions respectivement semblables à $x_1 x_2$ et $x_3 x_4$. On a, effectivement,

$$x_3 x_4 (x_1 + x_2) + x_1 x_2 (x_3 + x_4) = -r,$$

ou

$$z_2 (x_1 + x_2) + z_1 (x_3 + x_4) = -r;$$

d'ailleurs

$$(x_1 + x_2) + (x_3 + x_4) = -p,$$

donc

$$x_1 + x_2 = \frac{r - pz_1}{z_2 - z_1}, \quad x_3 + x_4 = \frac{pz_2 - r}{z_2 - z_1}.$$

Connaissant $x_1 + x_2$ et $x_1 x_2$, $x_3 + x_4$ et $x_3 x_4$, on formera deux équations du second degré, ayant pour racines, la première, x_1 et x_2, la seconde, x_3 et x_4, et le problème peut être considéré comme résolu.

On résout plus facilement l'équation du quatrième degré, en prenant une résolvante dont la racine soit une fonction linéaire des racines de l'équation proposée, ayant six valeurs égales deux à deux et de signes contraires.

Soit

$$t = x_1 + x_2 - x_3 - x_4;$$

cette fonction, ayant six valeurs, dépendra d'une équation du sixième degré : mais parce que ces valeurs de t sont égales deux à deux et de signes contraires, l'équation s'abaissera au troisième degré, en posant

$$t^2 = \theta.$$

On peut former directement l'équation en θ, puisqu'on connaît la composition de ses racines ; mais on peut aussi la déduire de la résolvante (3) en y. Il est facile, en effet, de voir que l'on a

$$y = \frac{\theta - p^2 + 4q}{4},$$

et la résolvante en θ est

$$(5)\ \left\{\begin{array}{l}\theta^3 - (3p^2 - 8q)\theta^2 + (3p^4 - 16p^2q + 16q^2 + 16pr - 64s)\theta \\ \quad - (p^3 - 4pq + 8r)^2 = 0.\end{array}\right.$$

On pourrait exprimer les quatre racines x_1, x_2, x_3, x_4 de la proposée, à l'aide d'une seule des racines θ de cette équation ; mais on obtient des résultats plus simples en employant les trois racines.

Soient $\theta_1, \theta_2, \theta_3$ les trois racines de l'équation (5), on aura

$$(6)\quad \left\{\begin{array}{l} x_1 + x_2 - x_3 - x_4 = \sqrt{\theta_1}, \\ x_1 + x_3 - x_2 - x_4 = \sqrt{\theta_2}, \\ x_1 + x_4 - x_2 - x_3 = \sqrt{\theta_3}; \end{array}\right.$$

d'ailleurs

$$(7)\quad x_1 + x_2 + x_3 + x_4 = -p,$$

et les équations (6) et (7), qui sont du premier degré, donneront les valeurs suivantes des quatre racines

$$x_1 = \frac{-p + \sqrt{\theta_1} + \sqrt{\theta_2} + \sqrt{\theta_3}}{4},$$

$$x_2 = \frac{-p + \sqrt{\theta_1} - \sqrt{\theta_2} - \sqrt{\theta_3}}{4},$$

$$x_3 = \frac{-p - \sqrt{\theta_1} + \sqrt{\theta_2} - \sqrt{\theta_3}}{4},$$

$$x_4 = \frac{-p - \sqrt{\theta_1} - \sqrt{\theta_2} + \sqrt{\theta_3}}{4}.$$

Ces quatre racines peuvent être représentées par la formule unique

$$(8) \qquad x = \frac{-p + \sqrt{\theta_1} + \sqrt{\theta_2} + \sqrt{\theta_3}}{4},$$

puisque chaque radical a deux valeurs égales et de signes contraires. Mais ici se présente une difficulté, car l'expression de x, donnée par l'équation (8), a huit valeurs, tandis que l'équation proposée ne peut avoir que quatre racines. Il est aisé de faire disparaître cette ambiguïté. En effet, on peut prendre à volonté l'une des deux valeurs de $\sqrt{\theta_1}$ et $\sqrt{\theta_2}$; mais quand on a fixé ces valeurs, celle du troisième radical $\sqrt{\theta_3}$ se trouve par cela même déterminée. En effet, en multipliant les trois équations (6), on trouve

$$\begin{aligned}
\sqrt{\theta_1}\sqrt{\theta_2}\sqrt{\theta_3} &= (x_1^3 + x_2^3 + x_3^3 + x_4^3) \\
&\quad + 2(x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4) \\
&\quad - x_1(x_2^2 + x_3^2 + x_4^2) - x_2(x_1^2 + x_3^2 + x_4^2) \\
&\quad - x_3(x_1^2 + x_2^2 + x_4^2) - x_4(x_1^2 + x_2^2 + x_3^2) \\
&= 2\sum x_1^3 + 2\sum x_1x_2x_3 - \sum x_1 \sum x_1^2 \\
&= -p^3 + 4pq - 8r,
\end{aligned}$$

d'où

$$\sqrt{\theta_3} = \frac{-p^3 + 4pq - 8r}{\sqrt{\theta_1}\sqrt{\theta_2}}.$$

Il résulte de là que la valeur de x, donnée par l'équation (8), a précisément quatre valeurs, et qu'elle représente bien, en conséquence, les quatre racines de l'équation proposée.

Remarque. — Il est important de remarquer que le succès des méthodes de Ferrari et de Lagrange est dû à cette seule circonstance, *que l'on peut former des fonctions de quatre lettres, qui n'aient que trois valeurs.*

Méthode de Descartes.

Cette méthode consiste à identifier l'équation proposée

$$x^4 + px^3 + qx^2 + rx + s = 0,$$

avec cette autre

$$(x^2 + fx + g)(x^2 + f'x + g') = 0,$$

dont les racines peuvent être considérées comme connues.

Au lieu d'employer la méthode des coefficients indéterminés, comme fait Descartes, on peut exprimer que $x^2 + fx + g$ est un diviseur du premier membre de l'équation proposée, en effectuant la division, et égalant à zéro les deux termes du reste qui est du premier degré en x. On obtient ainsi deux équations entre les deux inconnues f et g, et en éliminant g ou f, on a une équation du sixième degré qu'on ramène aisément au troisième, et qu'on peut considérer comme une résolvante de l'équation proposée. Cette méthode ne diffère pas, au fond, de celles que nous avons d'abord exposées ; car si l'on connaît une valeur de g ou de f, c'est-à-dire $x_1 x_2$ ou $x_1 + x_2$, on connaîtra également $x_3 x_4$ ou $x_3 + x_4$,

et la résolution de l'équation proposée s'en déduira comme nous l'avons montré précédemment.

Méthodes de Tschirnaüs et d'Euler.

Je n'ajouterai rien à ce que j'ai dit dans une précédente leçon au sujet de la méthode de Tschirnaüs, qui ramène l'équation

$$x^4 + px^3 + qx^2 + rx + s = 0$$

à la forme bicarrée, en employant la transformation

$$y = a + bx + x^2,$$

et disposant convenablement des indéterminées a et b.

La méthode d'Euler consiste à éliminer y entre les deux équations

$$x = a + by + cy^2 + dy^3,$$

$$y^4 = e,$$

et à identifier l'équation finale en x avec la proposée, dont les racines seront alors données par la formule

$$x = a + b\sqrt[4]{e} + c\left(\sqrt[4]{e}\right)^2 + d\left(\sqrt[4]{e}\right)^3.$$

Tout revient donc à déterminer les valeurs des indéterminées a, b, c, d, e, dont l'une peut être choisie arbitrairement.

DIX-HUITIÈME LEÇON.

Sur la résolution algébrique des équations. — Des équations de degré premier. — Des équations de degré non premier.

Sur la résolution algébrique des équations.

Toutes les méthodes connues que les géomètres ont essayé d'appliquer à la résolution algébrique des équations, et il en serait nécessairement de même des nouvelles qu'on pourrait imaginer, reviennent à faire dépendre la résolution de l'équation proposée de celle d'une autre équation plus facile à résoudre, et dont les racines sont des fonctions de celles de la proposée.

C'est ainsi que nous avons pu résoudre l'équation du troisième degré, en déterminant la valeur d'une fonction linéaire de ses racines x_1, x_2, x_3,

$$t = x_1 + \alpha x_2 + \alpha^2 x_3,$$

α désignant l'une des racines imaginaires de l'équation $x^3 = 1$. Le cube t^3 de cette fonction ne peut prendre que deux valeurs distinctes par les permutations des racines x_1, x_2, x_3, et dépend, par conséquent, d'une équation du second degré.

De même, nous avons résolu l'équation du quatrième degré en déterminant la valeur de l'une des deux fonctions suivantes de ses racines x_1, x_2, x_3, x_4,

$$y = x_1 x_2 + x_3 x_4,$$
$$t = x_1 - x_2 + x_3 - x_4.$$

La première de ces deux fonctions ne peut acquérir que trois valeurs, et dépend, par conséquent, d'une équation

du troisième degré, qu'on sait résoudre; la seconde peut prendre six valeurs, et dépend d'une équation du sixième degré, mais qu'on peut abaisser au troisième, parce qu'elle ne contient que des puissances paires de l'inconnue. Nous avons vu, dans la leçon précédente, que la résolvante en t conduit plus aisément que celle en y à la résolution de la proposée; elle a aussi cet avantage que la résolution de l'équation du quatrième degré, qu'on en déduit, présente la plus complète analogie avec celle de l'équation du troisième degré. La fonction t peut, en effet, s'écrire ainsi :

$$t = x_1 + \alpha x_2 + \alpha^2 x_3 + \alpha^3 x_4,$$

α désignant la racine réelle -1 de l'équation $x^4 = 1$.

Dans les *Mémoires de l'Académie de Berlin* (années 1770 et 1771) (*), Lagrange, prenant pour point de départ les résultats qui précèdent, a cherché à opérer la résolution de l'équation générale de degré m dont x_1, x_2, $x_3, \ldots, x_m$ sont les m racines, en employant une fonction de la forme

$$t = x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{m-2} x_{m-1} + \alpha^{m-1} x_m,$$

où α désigne une racine de l'équation $x^m = 1$.

Quoique ces recherches de Lagrange ne l'aient pas conduit à la résolution des équations générales d'un degré supérieur au quatrième, les développements qu'il a donnés à ce sujet présentent assez d'intérêt pour qu'il semble utile de les exposer ici.

Nous suivrons la marche tracée par l'illustre auteur, et nous distinguerons avec lui le cas où le degré de l'équation est un nombre premier, et celui où il est un nombre composé.

(*) Lagrange a présenté un extrait de son Mémoire dans la note XIII de son *Traité de la Résolution des équations numériques*, 3e édition, page 242.

Des équations de degré premier.

Soient

$$x_1,\ x_2,\ x_3, \ldots,\ x_m$$

les m racines d'une équation

$$(1) \qquad V = 0,$$

de degré premier m, α une racine quelconque de l'équation $x^m = 1$, et posons

$$(2) \qquad t = x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{m-1} x_m.$$

Si α n'est pas égal à 1, m étant premier, les puissances de α, savoir

$$1,\ \alpha,\ \alpha^2, \ldots,\ \alpha^{m-1},$$

sont les m racines de l'équation $x^m = 1$, et, par conséquent, sont toutes distinctes. Il résulte de là que la fonction t prendra $1.2.3\ldots m$ valeurs distinctes, si l'on y permute les m racines x_1, x_2, etc.; cette fonction dépend donc d'une équation du degré

$$1.2.3\ldots m,$$

qu'on peut former par la méthode exposée dans la deuxième leçon, puisqu'on connaît la composition de ses racines.

Nous allons démontrer que *la résolution de cette équation de degré* $1.2.3\ldots m$, *peut se ramener à la résolution d'une équation du degré* $m-1$, *dont les coefficients dépendent d'une équation du degré* $1.2.3\ldots(m-2)$.

Multiplions successivement l'expression de t par $\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{m-1}$, et rabaissons les exposants de α au-dessous de m, à l'aide de la relation $\alpha^{m+n} = \alpha^n$, on a

$$\begin{aligned}
t &= x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{m-1} x_m,\\
\alpha t &= \alpha x_1 + \alpha^2 x_2 + \alpha^3 x_3 + \ldots + x_m,\\
\alpha^2 t &= \alpha^2 x_1 + \alpha^3 x_2 + \alpha^4 x_3 + \ldots + \alpha x_m,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\alpha^{m-1} t &= \alpha^{m-1} x_1 + x_2 + \alpha x_3 + \ldots + \alpha^{m-2} x_m,
\end{aligned}$$

ou, en ordonnant par rapport aux puissances de α.

$$(3)\quad\left\{\begin{array}{l} t = x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{m-1} x_m, \\ \alpha t = x_m + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{m-1} x_{m-1}, \\ \alpha^2 t = x_{m-1} + \alpha x_m + \alpha^2 x_1 + \ldots + \alpha^{m-1} x_{m-2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha^{m-1} t = x_2 + \alpha x_3 + \alpha^2 x_4 + \ldots + \alpha^{m-1} x_1. \end{array}\right.$$

On voit que chacune des quantités

$$t,\ \alpha t,\ \alpha^2 t, \ldots,\ \alpha^{m-1} t$$

se déduit de la précédente par la substitution

$$\begin{pmatrix} x_1, & x_2, \ldots, & x_m \\ x_m, & x_1, \ldots & x_{m-1} \end{pmatrix},$$

et, par conséquent, chacune des racines x_1, x_2, etc., occupe, dans les seconds membres des équations (3), toutes les places. Par exemple, x_1 est à la première place dans t, à la deuxième dans αt, etc., à la dernière place dans $\alpha^{m-1} t$; on aura donc les $1.2.3\ldots m$ valeurs de t, en faisant subir aux $m-1$ lettres $x_2, x_3, \ldots, x_m$, dans les seconds membres des équations (3), les $1.2.3\ldots(m-1)$ permutations dont elles sont susceptibles, sans changer la place de x_1. Et si l'on fait, pour abréger,

$$\mu = 1.2.3\ldots(m-1),$$

et que l'on désigne par

$$t_1,\ t_2,\ t_3, \ldots, t_\mu$$

les μ valeurs que prend t, quand on y permute les $m-1$ lettres $x_2, x_3, \ldots, x_m$, les $1.2.3\ldots m$ racines de l'équa-

tion en t seront

$$\begin{array}{l} t_1,\ \alpha t_1,\ \alpha^2 t_1,\ \ldots,\ \alpha^{m-1} t_1,\\ t_2,\ \alpha t_2,\ \alpha^2 t_2,\ \ldots,\ \alpha^{m-1} t_2,\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ t_\mu,\ \alpha t_\mu,\ \alpha^2 t_\mu,\ \ldots,\ \alpha^{m-1} t_\mu; \end{array}$$

on a d'ailleurs

$$(t - t_p)(t - \alpha t_p)\ldots(t - \alpha^{m-1} t_p) = t^m - t_p^m,$$

l'équation en t sera donc

$$\left(t^m - t_1^m\right)\left(t^m - t_2^m\right)\cdots\left(t^m - t_\mu^m\right) = 0.$$

On voit que cette équation ne contient que des puissances de t dont les exposants sont divisibles par m, et qu'elle s'abaissera au degré $\mu = 1.2.3\ldots(m-1)$, en posant

$$t^m = \theta.$$

L'expression de θ est

$$(4)\qquad \theta = (x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{m-1} x_m)^m,$$

et l'on en déduira celle des μ racines de l'équation en θ, en permutant, de toutes les manières possibles, les $m-1$ lettres x_2, x_3, ..., x_m, sans changer x_1 de place. Or, parmi ces permutations, qui servent à déduire toutes les valeurs de θ de l'une d'entre elles, il en est qui méritent surtout de fixer l'attention, parce qu'elles équivalent au simple changement de α en α^2, α^3, ..., α^{m-1}. En effet, m étant un nombre premier, si dans la série

$$\alpha,\ \alpha^2,\ \ldots,\ \alpha^{m-1}$$

on remplace α par α^n, n étant $< m$, on reproduira les mêmes racines, mais dans un ordre différent. La substitution à α, de l'une de ses puissances, équivaut donc à

un certain changement des puissances de α entre elles dans l'expression de θ, et, par suite, à un certain changement des racines $x_2, x_3, \ldots, x_m$ entre elles.

Remplaçons donc α, dans l'expression (4) de θ, par chacune de ses puissances $\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{m-1}$, rabaissons les exposants de α au-dessous de m, et ordonnons, par rapport aux puissances de α, la fonction dont la puissance m est égale à θ; désignons enfin par

$$\theta_1, \ \theta_2, \ \theta_3, \ldots, \ \theta_{m-1},$$

les $m-1$ valeurs de θ ainsi obtenues : il est évident que x_2, qui occupe la deuxième place dans θ_1, aura la troisième dans θ_2, la quatrième dans θ_3, etc., la dernière dans θ_{m-1}, et l'on aura

$$(5)\quad \left\{\begin{array}{l} \theta_1 = (x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \ldots \alpha^{m-1} x_m)^m, \\ \theta_2 = \left(x_1 + \alpha x_{\frac{m+3}{2}} + \alpha^2 x_2 + \ldots\ldots\ldots\ldots\right)^m, \\ \theta_3 = (x_1 + \ldots\ldots\ldots\ldots + \alpha^3 x_2 + \ldots\ldots)^m, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \theta_{m-1} = (x_1 + \ldots\ldots\ldots\ldots\ldots\ldots + \alpha^{m-1} x_2)^m. \end{array}\right.$$

Voilà donc $m-1$ valeurs de θ dans lesquelles x_2 occupe successivement la seconde, la troisième, etc., la dernière place, en sorte qu'il suffira, pour avoir les $1.2.3\ldots(m-1)$ valeurs de θ, de faire, dans chacune des $m-1$ valeurs que nous venons d'écrire, les $1.2.3\ldots(m-2)$ permutations des lettres $x_3, x_4, \ldots, x_m$, les unes dans les autres, sans changer la place ni de x_1 ni de x_2. On déduira, en effet, par ce moyen $1.2.3\ldots(m-2)$ valeurs de θ, de chacune des valeurs (5), ce qui fera en tout $1.2.3\ldots(m-1)$.

Si maintenant on considère l'équation de degré $m-1$

$$(\theta - \theta_1)(\theta - \theta_2)\ldots(\theta - \theta_{m-1}) = 0,$$

ou

$$(6) \qquad \theta^{m-1} + p_1\theta^{m-2} + p_2\theta^{m-3} + \ldots + p_{m-1}\theta + p_m = 0,$$

qui a pour racines les quantités $\theta_1, \theta_2, \ldots, \theta_{m-1}$; je dis que les coefficients p_1, p_2, etc., de cette équation ne dépendent que d'une équation du degré $1.2.3\ldots(m-2)$, en sorte que l'équation du degré $1.2.3\ldots(m-1)$, qui a pour racines toutes les valeurs de θ, se décomposera en $1.2.3\ldots(m-2)$ facteurs du degré $m-1$, à l'aide d'une seule équation du degré $1.2.3\ldots(m-2)$.

D'abord il est facile de voir que toute fonction symétrique des quantités $\theta_1, \theta_2, \theta_3, \ldots, \theta_{m-1}$, ne peut acquérir que $1.2.3\ldots(m-2)$ valeurs, par les $1.2.3\ldots(m-2)$ permutations des lettres $x_3, x_4, \ldots, x_m$.

En effet, si l'on remplace α par l'une quelconque de ses puissances, α^{n-1}, les quantités $\theta_1, \theta_2, \ldots, \theta_{m-1}$ ne feront que s'échanger les unes dans les autres, car θ_2, θ_3, etc., se déduisant de θ_1 par les changements de α en α^2, α^3, etc., on peut les représenter par

$$(7) \qquad \theta(\alpha),\ \theta(\alpha^2),\ \theta(\alpha^3), \ldots,\ \theta(\alpha^{m-1});$$

et ces quantités (7) sont les mêmes, à l'ordre près, que les suivantes

$$(8) \qquad \theta(\alpha^{n-1}),\ \theta[\alpha^{2(n-1)}], \ldots,\ \theta[\alpha^{(m-1)(n-1)}],$$

qui se déduisent de la première d'entre elles de la même manière que les quantités (7), c'est-à-dire par les changements de α en $\alpha^2, \alpha^3, \ldots, \alpha^{m-1}$.

Maintenant, le changement de α en α^{n-1} dans θ_1 ou $\theta(\alpha)$ équivaut à une certaine permutation des lettres x_2, $x_3, \ldots, x_m$, qui amène x_2 à la place de x_n; d'où il suit que les quantités (8) se déduiront (à l'ordre près) des quantités (7) par la même substitution. Il y a donc, en un mot, des substitutions pouvant amener x_2 à la place

de l'une quelconque des lettres suivantes $x_3, x_4, \ldots, x_m$, et par lesquelles les quantités $\theta_1, \theta_2, \ldots, \theta_{m-1}$ ne font que s'échanger les unes dans les autres. Par conséquent, ces substitutions ne changeront pas la valeur d'une fonction symétrique des quantités $\theta_1, \theta_2, \ldots, \theta_{m-1}$.

Cela étant, supposons qu'on veuille appliquer à une fonction symétrique de θ_1, θ_2, etc., une substitution quelconque devant amener x_2 à la place de x_n, on pourra commencer par amener x_2 à la place de x_n par une substitution qui ne change en rien la valeur de la fonction symétrique, ensuite il n'y aura plus qu'à opérer une certaine substitution sur les $m-2$ lettres $x_3, x_4, \ldots, x_m$, la seule qui puisse changer la valeur de la fonction symétrique. Ainsi, la place de x_2 pouvant être fixée à volonté dans une fonction symétrique de θ_1, θ_2, etc., une pareille fonction ne saurait avoir que les $1.2.3\ldots(m-2)$ valeurs résultant des permutations des $m-2$ lettres $x_3, x_4, \ldots, x_m$.

D'après ce qui précède, chacun des coefficients p_1, p_2, etc., de l'équation (6) dépend d'une équation du degré $1.2.3\ldots(m-2)$, et l'on pourra former chacune de ces équations par la méthode exposée dans la deuxième leçon, puisqu'on connaît la composition de leurs racines. Mais on aperçoit immédiatement que tous ces coefficients p_1, p_2, etc., ne dépendent que d'une seule équation du degré $1.2.3\ldots(m-2)$, car ce sont évidemment des fonctions semblables des racines $x_1, x_2, \ldots, x_m$ de l'équation proposée, et si l'on se donne la valeur de l'un d'eux, celles de tous les autres s'en déduiront rationnellement.

Voici comment on peut opérer pour former l'équation dont p_1 dépend, et pour exprimer en fonction de p_1 les autres coefficients p_2, p_3, etc. On calculera l'équation de degré $1.2.3\ldots(m-1)$, qui a pour racines toutes les valeurs de θ, et dont les coefficients, fonctions invariables

des racines de la proposée, sont exprimables rationnellement par ses coefficients. Le premier membre de l'équation (6) étant un diviseur du premier membre de cette équation complète en θ, on fera la division à la manière ordinaire, et on égalera à zéro les $m-1$ termes du reste. Les $m-2$ premières des équations ainsi obtenues serviront à déterminer les coefficients p_2, p_3, etc., en fonction de p_1, et on aura ensuite l'équation en p_1 de degré $1.2.3\ldots(m-2)$, en remplaçant dans la $(m-1)^{ième}$, p_2, p_3, etc., par les valeurs qu'on aura trouvées.

Lagrange a cherché à simplifier les calculs, presque impraticables dès le cinquième degré, auxquels conduit l'application de la théorie précédente; il a effectivement imaginé un artifice ingénieux pour exprimer les coefficients de l'équation (6), en fonction des racines x_1, x_2, etc. Je vais le rapporter ici.

Pour avoir l'expression de θ, il faut élever à la puissance m la quantité

$$x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{m-1} x_m;$$

en faisant ce calcul, et ayant soin de rabaisser les exposants de α au-dessous de m, on a un résultat de la forme

$$\theta = \xi_0 + \alpha\xi_1 + \alpha^2\xi_2 + \ldots + \alpha^{m-1}\xi_{m-1}. \tag{9}$$

L'équation (9) donne les valeurs de $\theta_1, \theta_2, \ldots, \theta_{m-1}$, en substituant à α chacune des racines imaginaires α, 6, $\gamma, \ldots, \omega$ de l'équation $x^m = 1$. En outre, si l'on remplace α par 1, le second membre de l'équation (9) a pour valeur $(x_1 + x_2 + \ldots + x_m)^m$ ou A^m, en désignant par A la somme connue des racines de l'équation proposée (1). On a donc,

$$\begin{aligned}
A^m &= \xi_0 + \xi_1 + \xi_2 + \ldots\ldots\ldots\ldots + \xi_{m-1},\\
\theta_1 &= \xi_0 + \alpha\xi_1 + \alpha^2\xi_2 + \ldots + \alpha^{m-1}\xi_{m-1},\\
\theta_2 &= \xi_0 + 6\xi_1 + 6^2\xi_2 + \ldots + 6^{m-1}\xi_{m-1},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\theta_{m-1} &= \xi_0 + \omega\xi_1 + \omega^2\xi_2 + \ldots + \omega^{m-1}\xi_{m-1}.
\end{aligned}$$

Ajoutons ces équations et désignons par s_1 la somme des racines de l'équation (6), on aura, d'après les propriétés des racines α, 6, etc.,

$$A^m + s_1 = m\xi_0,$$

ou

$$s_1 = m\xi_0 - A^m.$$

Désignons généralement par s_n la somme des puissances n des racines de l'équation (6); élevons l'équation (9) à la puissance n, et rabaissant les exposants de α au-dessous de m, représentons le résultat par

$$\theta^n = \xi_0^{(n)} + \alpha\xi_1^{(n)} + \alpha^2\xi_2^{(n)} + \ldots + \alpha^{m-1}\xi_{m-1}^{(n)};$$

remplaçons ensuite α successivement par $1, \alpha, 6, \ldots, \omega$, et ajoutons les résultats, on aura

$$A^{mn} + s_n = m\,\xi_0^{(n)},$$

ou

$$s_n = m\,\xi_0^{(n)} - A^{mn}.$$

On pourra calculer de cette manière, en fonction des racines $x_1, x_2, \ldots, x_m$, les sommes $s_2, s_3, \ldots, s_{m-1}$, et l'on en déduira ensuite les valeurs suivantes des coefficients p_1, p_2, etc., de l'équation (6)

$$p_1 = -(m\xi_0 - A^m),$$

$$p_2 = -\frac{(m\xi_0 - A^m)^2}{2} - \frac{(m\xi_0^{(2)} - A^{2m})}{2},$$

$$p_3 = -\frac{(m\xi_0 - A^m)^3}{2.3} + \frac{(m\xi_0 - A^m)(m\xi_0^{(2)} - A^{2m})}{2} - \frac{(m\xi_0^{(3)} - A^{3m})}{3},$$

. . . .
. . . .

Voilà donc les coefficients p_1, p_2, etc., de l'équation (6) exprimés en fonction des racines $x_1, x_2, \ldots, x_m$ de l'équation proposée, et si l'on fait dans l'expression de l'un d'eux, de p_1, par exemple, toutes les permutations possibles, on ne trouvera que $1.2.3\ldots(m-2)$ valeurs distinctes. On pourra ainsi former directement l'équation en p_1, et l'on exprimera ensuite les valeurs des autres coefficients en fonction rationnelle de p_1, par le procédé indiqué plus haut.

Si l'on connaît un seul système de valeurs des coefficients p_1, p_2, etc., et si l'on peut résoudre l'équation en θ correspondante de degré $m-1$, la résolution de l'équation proposée (1) s'ensuivra immédiatement, comme nous allons l'expliquer.

Dans l'hypothèse où nous nous plaçons, les quantités $\theta_1, \theta_2, \ldots, \theta_{m-1}$ sont connues : les équations (5) donnent, en mettant $\alpha, 6, \gamma, \ldots, \omega$ au lieu de $\alpha, \alpha^2, \ldots, \alpha^{m-1}$,

$$(10)\quad \begin{cases} x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{m-1} x_m = \sqrt[m]{\theta_1}, \\ x_1 + 6 x_2 + 6^2 x_3 + \ldots + 6^{m-1} x_m = \sqrt[m]{\theta_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_1 + \omega x_2 + \omega^2 x_3 + \ldots + \omega^{m-1} x_m = \sqrt[m]{\theta_{m-1}}, \end{cases}$$

on a d'ailleurs

$$x_1 + x_2 + x_3 + \ldots + x_m = \text{A};$$

donc, en ajoutant ces équations, et ayant égard aux propriétés des racines α, 6, etc., on a

$$(11)\qquad x_1 = \frac{\text{A} + \sqrt[m]{\theta_1} + \sqrt[m]{\theta_2} + \ldots + \sqrt[m]{\theta_{m-1}}}{m};$$

ajoutant aussi ces mêmes équations respectivement mul-

tipliées par $\alpha^n, \delta^n, \ldots, \omega^n$ et 1, on a

$$(12)\quad x_{m-n+1} = \frac{A + \alpha^n \sqrt[m]{\theta_1} + \mathrm{6}^n \sqrt[n]{\theta_2} + \ldots + \omega^n \sqrt[n]{\theta_{m-1}}}{m}.$$

Mais comme rien ne détermine celle des valeurs de chaque radical qu'il faut prendre, le second membre de l'équation (12) est absolument identique au second membre de l'équation (11). Aussi doit-on se borner à dire que les m racines de l'équation proposée sont données par la formule unique

$$(13)\quad x = \frac{A + \sqrt[m]{\theta_1} + \sqrt[m]{\theta_2} + \ldots + \sqrt[m]{\theta_{m-1}}}{m}.$$

A la vérité, cette formule, à cause de la multiplicité des valeurs de chaque radical, donne pour x un nombre de valeurs égal à m^{m-1}; mais on peut faire disparaître l'ambiguïté qui en résulte. En effet, les premiers membres des équations (10) sont des fonctions semblables des racines x_1, x_2, etc.; on pourra donc, si l'on se donne l'un d'eux, en déduire rationnellement tous les autres. Ainsi, on pourra exprimer $\sqrt[m]{\theta_2}, \sqrt[m]{\theta_3}, \ldots, \sqrt[m]{\theta_{m-1}}$ rationnellement en fonction de $\sqrt[m]{\theta_1}$, et la formule (13) ne donnera alors pour x que m valeurs, comme cela doit être.

Par cette méthode, la résolution de l'équation du cinquième degré se ramène à celle d'une équation du quatrième degré, dont les coefficients dépendent d'une équation du sixième.

Des équations de degré non premier.

On voit aisément que l'analyse précédente ne peut s'appliquer aux équations dont le degré est un nombre composé. En effet, les quantités θ_1, θ_2, etc., que nous

avons déduites de θ en remplaçant α successivement par x, α^2, α^3, etc., ne sont plus toutes des racines de l'équation résolvante en θ, parce qu'alors, en remplaçant α par l'une de ces puissances dans la série

$$x,\ x^2,\ x^3,\ldots,$$

on ne reproduit pas nécessairement ces mêmes quantités, lors même que α serait une racine primitive de l'équation $x^m = 1$. Aussi Lagrange a-t-il cherché une autre méthode : celle qu'il a suivie revient, en dernière analyse, à décomposer l'équation proposée

$$(1) \qquad V = 0,$$

de degré $m = np$, n étant un nombre premier, en n équations du degré p; et cette méthode n'exige pour cela que la résolution d'une équation de degré

$$\frac{1.2\ldots m}{(n-1)n\,(1.2\ldots p)^n},$$

et celle d'une équation de degré $n-1$, tandis que si l'on cherchait à faire la décomposition par la méthode ordinaire, il faudrait résoudre une équation du degré

$$\frac{m(m-1)\ldots(m-p+1)}{1.2\ldots p}.$$

Cette décomposition de l'équation (1) en n équations du degré p une fois faite, on pourra appliquer à chacune de ces dernières la méthode exposée précédemment, si p est un nombre premier. Dans le cas contraire, si $p = n'p'$, n' étant un nombre premier, on ramènera la résolution de chaque équation de degré p à celle de n' équations du degré p', en opérant de la même manière que pour la proposée; et ainsi de suite. Entrons maintenant dans les détails.

Soit $m = np$, n étant un nombre premier, et posons, comme précédemment,

$$t = x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{m-1} x_m,$$

$x_1, x_2, \ldots, x_m$ désignant les m racines de l'équation (1) et α une racine de $x^m = 1$, mais qui appartienne aussi à l'équation $x^n = 1$. Alors, comme on a généralement

$$\alpha^{n+k} = \alpha^k,$$

la valeur précédente de t pourra s'écrire comme il suit :

$$\begin{aligned} t = & \left[x_1 + x_{n+1} + x_{2n+1} + \ldots + x_{(p-1)n+1}\right] \\ & + \alpha\left[x_2 + x_{n+2} + x_{2n+2} + \ldots + x_{(p-1)n+2}\right] \\ & + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & + \alpha^{n-1}\left[x_n + x_{2n} + x_{3n} + \ldots\ldots + x_{pn}\right], \end{aligned}$$

ou

$$t = X_1 + \alpha X_2 + \alpha^2 X_3 + \ldots + \alpha^{n-1} X_n,$$

en faisant, pour abréger,

$$(2)\quad \left\{ \begin{aligned} X_1 &= x_1 + x_{n+1} + x_{2n+1} + \ldots + x_{(p-1)n+1}, \\ X_2 &= x_2 + x_{n+2} + x_{2n+2} + \ldots + x_{(p-1)n+2}, \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_n &= x_n + x_{2n} + x_{3n} + \ldots\ldots\ldots + x_{pn}. \end{aligned} \right.$$

Soit

$$(3)\qquad W = 0$$

l'équation qui a pour racines $X_1, X_2, \ldots, X_n$; on pourra appliquer à cette équation (3) la méthode exposée précédemment pour les équations de degré premier. Faisons $\theta = t^n$, ou

$$(4)\qquad \theta = (X_1 + \alpha X_2 + \ldots + \alpha^{n-1} X_n)^n,$$

θ dépend d'une équation du degré $1.2.3\ldots(n-1)$ dont les coefficients peuvent s'exprimer rationnellement par ceux de l'équation (3); et si l'on représente par $\theta_1, \theta_2, \ldots, \theta_{n-1}$ les $n-1$ valeurs que prend θ, en remplaçant α par les $n-1$ racines imaginaires de $x^n=1$, on peut former l'équation en θ de degré $n-1$ qui a ces $n-1$ valeurs de θ pour racines : représentons cette équation par

$$(5) \qquad \theta^{n-1}+p_1\theta^{n-2}+p_2\theta^{n-3}+\ldots+p_{n-1}\theta+p_n=0;$$

ses coefficients p_1, p_2, etc., dépendent d'une seule équation de degré $1.2.3\ldots(n-2)$ dont les coefficients s'expriment rationnellement par ceux de l'équation (3), ainsi que nous l'avons établi précédemment.

Soient y l'un quelconque des coefficients p_1, p_2, etc., et

$$(6) \qquad f(y)=0$$

l'équation de degré $1.2.3\ldots(n-2)$ dont y dépend. Les coefficients de cette équation (6) sont exprimables rationnellement par ceux de l'équation (3), mais ces derniers ne sont pas connus, il n'y a que ceux de l'équation (1) qui le soient; voici comment on peut former une équation en y dont les coefficients soient exprimés par les quantités connues.

$f(y)$ est une fonction de y qui contient symétriquement les quantités $X_1, X_2, \ldots, X_n$, et, en remplaçant X_1, X_2, etc., par leurs valeurs tirées des équations (2), $f(y)$ deviendra une fonction non symétrique des racines $x_1, x_2, \ldots, x_m$ de l'équation (1). Faisons dans $f(y)$ toutes les permutations des racines $x_1, x_2, \ldots, x_m$, et désignons par

$$f_1(y), \quad f_2(y), \ldots, \; f_\mu(y)$$

les μ valeurs distinctes que prend ainsi $f(y)$; le produit de toutes ces valeurs est une fonction symétrique des ra-

cines $x_1, x_2, \ldots, x_m$ de la proposée, exprimable rationnellement par ses coefficients. On a donc, pour déterminer y, l'équation

$$(7) \qquad f_1(y)\, f_2(y)\, f_3(y) \ldots f_\mu(y) = 0,$$

dont les coefficients peuvent être considérés comme connus.

Le degré de cette équation (7) est $1.2.3\ldots(n-2)\times\mu$, μ désignant le nombre des valeurs distinctes de $f(y)$, quand on y permute les lettres $x_1, x_2, \ldots, x_m$; nous savons que ce nombre μ est un diviseur du produit $1.2.3\ldots m$ (onzième leçon), et si l'on fait

$$\mu = \frac{1.2.3\ldots m}{\nu},$$

ν sera le nombre des permutations des lettres $x_1, x_2, \ldots, x_m$ qui ne font pas changer la fonction $f(y)$. Or $f(y)$ ne change pas en permutant, les unes dans les autres, les lettres qui composent respectivement $X_1, X_2, \ldots, X_n$, non plus qu'en échangeant les quantités X_1, X_2, etc., les unes dans les autres; mais toute permutation des lettres x_1, x_2, etc., qui fait passer quelques-unes des lettres de X_1 ou X_2, ou, etc., dans l'une des autres fonctions, change évidemment la fonction $f(y)$. On conclut aisément de là que

$$\nu = (1.2.3\ldots p)^n.(1.2\ldots n),$$

et, par conséquent,

$$\mu = \frac{1.2.3\ldots m}{(1.2.3\ldots n)(1.2.3\ldots p)^n}.$$

Le degré de l'équation (7) est donc

$$1.2.3\ldots(n-2).\frac{1.2.3\ldots m}{(1.2.3\ldots n)(1.2\ldots p)^n},$$

ou

$$\frac{1.2.3\ldots m}{(n-1)n(1.2.3\ldots p)^n}.$$

Si l'on connaît une seule racine de l'équation (7) on aura un système de valeurs des coefficients

$$p_1,\ p_2,\ldots,\ p_{n-1}$$

de l'équation (5), car ces coefficients sont des fonctions semblables des racines de l'équation proposée, et, par conséquent, ils peuvent s'exprimer rationnellement en fonction de l'un quelconque d'entre eux et des quantités connues.

On résoudra ensuite l'équation (5), qui n'est que du degré $n-1$, et l'on aura alors aisément les racines de l'équation (4). Désignons, en effet, par

$$\theta_1,\ \theta_2,\ldots,\ \theta_{n-1}$$

les $n-1$ racines de l'équation (5); ces valeurs de θ étant précisément celles qu'on déduit de l'équation (4), en remplaçant α par chacune des racines imaginaires de $x^n=1$, on aura

$$X_1+\alpha X_2+\alpha^2 X_3+\ldots+\alpha^{n-1}X_n=\sqrt[n]{\theta_1},$$
$$X_1+6X_2+6^2 X_3+\ldots+6^{n-1}X_n=\sqrt[n]{\theta_2},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$X_1+\omega X_2+\omega^2 X_3+\ldots+\omega^{n-1}X_n=\sqrt[n]{\theta_{n-1}}.$$

D'ailleurs, la somme des racines $X_1, X_2,\ldots, X_n$ est connue, car elle est la même que celle des racines $x_1, x_2,\ldots, x_m$; en désignant donc par A cette somme, on aura

$$X_1+X_2+X_3+\ldots+X_n=A.$$

Des équations qui précèdent, on tire cette expression gé-

nérale des racines X_1, X_2, etc.,

$$X = \frac{A + \sqrt[n]{\theta_1} + \sqrt[n]{\theta_2} + \ldots + \sqrt[n]{\theta_{n-1}}}{n}.$$

Il ne reste plus, maintenant, qu'à trouver les racines x_1, x_2, etc., elles-mêmes; pour cela, on considérera l'équation qui a pour racines celles de la proposée dont la somme est X_1 ou X_2, etc., X_1 par exemple : soit

$$x^p - X_1 x^{p-1} + q_2 x^{p-2} + \ldots + q_{p-1} x + q_p = 0$$

cette équation, dont le premier membre est un diviseur du premier membre V de la proposée. On fera la division à la manière ordinaire, et on égalera à zéro les p termes du reste; on aura ainsi p équations dont les $p-1$ premières détermineront q_2, q_3, etc., en fonction de X_1, la dernière étant alors satisfaite d'elle-même. Il est évident, à priori, que q_2, q_3, etc., doivent s'exprimer rationnellement en fonction de X_1, puisque ce sont des fonctions semblables. On aura donc enfin, par ce moyen, les n équations de degré p, dans lesquelles peut se décomposer l'équation proposée.

Tel est le point où se trouve ramenée aujourd'hui la question de la résolution algébrique des équations. La fonction résolvante de Lagrange nous a donné la résolution des équations du troisième et du quatrième degré, mais elle n'est d'aucune utilité pour les équations générales de degré supérieur au quatrième, dont, au surplus, la résolution est aujourd'hui démontrée impossible. Toutefois nous verrons, dans une prochaine leçon, que la considération de cette fonction résolvante fournit la résolution algébrique d'une classe fort étendue d'équations de degrés quelconques.

A la même époque où Lagrange publiait, à Berlin, le

Mémoire dont nous venons de présenter les résultats principaux, Vandermonde s'occupait de la même question, et présentait, à l'Académie des Sciences de Paris, un beau Mémoire où, par des considérations différentes de celles de Lagrange, il arrivait pourtant aux mêmes conséquences. Je me borne ici à indiquer ce travail de Vandermonde, imprimé dans les *Mémoires de l'Académie des Sciences de Paris* (année 1771).

DIX-NEUVIÈME LEÇON.

Sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme. — Des substitutions circulaires. — Théorème de M. Cauchy. — Forme générale des fonctions qui n'ont que deux valeurs.

Sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme.

Le succès des méthodes exposées précédemment pour la résolution des équations générales du troisième et du quatrième degré est dû à cette seule circonstance, qu'on peut former des fonctions de trois lettres qui n'aient que deux valeurs, et des fonctions de quatre lettres qui n'en aient que trois. Et si l'on pouvait de même former des fonctions de cinq lettres n'ayant que quatre ou trois valeurs, on est fondé à penser que ces fonctions permettraient de résoudre l'équation générale du cinquième degré. On voit par là combien la question du nombre de valeurs qu'une fonction peut acquérir, quand on y permute les lettres qu'elle renferme, est liée intimement à la théorie des équations. Aussi plusieurs géomètres s'en sont-ils occupés; et quoiqu'ils aient laissé beaucoup à faire à leurs successeurs, ils ont pourtant obtenu quelques résultats intéressants que nous allons exposer.

Lagrange est le premier qui se soit occupé de cette question, en démontrant (*voir* onzième leçon) que *le nombre des valeurs d'une fonction de n lettres est toujours un diviseur du produit* $1.2.3\ldots n$.

Rufini, dans sa Théorie des équations, a considéré particulièrement les fonctions de cinq lettres, et il est parvenu à démontrer le théorème suivant :

Si une fonction de cinq variables a moins de cinq valeurs distinctes, elle ne peut en avoir plus de deux.

Ce théorème de Rufini a été généralisé ensuite et étendu aux fonctions de n lettres par Pietro Abatti. Ce géomètre a en effet démontré, dans le tome X des *Mémoires de la Société italienne*, que,

Si une fonction d'un nombre quelconque de variables, supérieur à quatre, a moins de cinq valeurs distinctes, elle ne peut en avoir plus de deux.

M. Cauchy, dans un Mémoire publié dans le tome X du *Journal de l'École Polytechnique*, est allé plus loin que les deux géomètres italiens. Il a prouvé qu'on pouvait, dans le théorème d'Abatti, substituer à la limite 5 le plus grand nombre premier contenu dans n. Ainsi, d'après M. Cauchy,

Si une fonction de n lettres a moins de p valeurs distinctes (p étant le plus grand nombre premier contenu dans n), elle ne peut en avoir plus de deux.

Et comme $p = n$, si n est premier, on a, en particulier, ce théorème :

Si une fonction de n lettres a moins de n valeurs distinctes, n étant un nombre premier, elle ne peut en avoir plus de deux.

M. Cauchy donne à entendre, dans son Mémoire, qu'il chercha à étendre le théorème précédent au cas où n n'est pas un nombre premier, mais il ne put y parvenir que dans le cas de $n = 6$. Il a, en effet, démontré que

Si une fonction de six lettres a moins de six valeurs distinctes, elle ne peut en avoir plus de deux.

Enfin M. Bertrand s'est occupé, dans ces dernières années, de cette même question, et il est parvenu à dé-

montrer généralement le théorème que M. Cauchy avait établi, avant lui, dans un cas particulier. Ainsi, d'après M. Bertrand,

Si une fonction de n lettres a moins de n valeurs distinctes, elle ne peut en avoir plus de deux.

La démonstration du théorème de M. Bertrand repose sur le *postulatum* suivant : *Si $n > 7$, il y a au moins un nombre premier p compris entre $n-2$ et $\frac{n}{2}$.* Ce *postulatum* serait sans doute très-difficile à démontrer, mais les Tables de nombres premiers ont permis d'en constater l'exactitude pour toutes les valeurs de n comprises entre 7 et 6000000, en sorte que le théorème de M. Bertrand se trouve démontré par lui, au moins pour les fonctions qui ont moins de 6000000 de variables.

La démonstration de M. Bertrand conduit à cet autre théorème, démontré auparavant par Abel pour les fonctions de cinq lettres :

Si une fonction de n lettres a n valeurs, elle est symétrique par rapport à $n-1$ lettres.

Dans une Note publiée dans le XXXIIe cahier du *Journal de l'École Polytechnique,* j'ai fait voir que si, entre $n-2$ et $\frac{n}{2}$, il n'y a aucun nombre premier, le théorème de M. Bertrand continue d'avoir lieu, pourvu que $\frac{n}{2}$ soit un nombre premier. La démonstration n'est en aucune façon modifiée, seulement on ne peut plus conclure ce corollaire que si une fonction de n lettres a n valeurs, elle est symétrique par rapport à $n-1$ lettres.

Cette remarque est importante, car il en résulte que le théorème de M. Bertrand comprend celui de M. Cauchy pour les fonctions de six lettres, et rend, par suite, inu-

tile la démonstration un peu compliquée de M. Cauchy. En effet, si $n = 6$, il n'y a aucun nombre premier entre $n - 2$ et $\frac{n}{2}$, mais $\frac{n}{2}$ ou 3 est un nombre premier.

M. Bertrand a démontré aussi un second théorème, mais moins important que le premier. Nous nous bornerons ici à l'énoncer, et nous renverrons à son Mémoire pour la démonstration (*). Voici ce théorème :

Si une fonction de n lettres, n étant > 9, a plus de n valeurs, elle en a au moins 2n.

Tels sont les résultats principaux acquis à la science dans cette théorie. Le problème général, qu'il serait intéressant de résoudre, consisterait à déterminer quels sont, parmi les diviseurs du produit $1.2.3\ldots n$, ceux qui peuvent représenter le nombre des valeurs d'une fonction de n lettres. On voit combien les théorèmes que nous venons d'indiquer sont loin de répondre, d'une manière complète, à cette question. Toutefois ces théorèmes suffisent pour l'objet qu'on doit avoir en vue dans la théorie des équations. Ainsi, en particulier, le théorème de Ruffini, s'il n'établit pas l'impossibilité de résoudre l'équation générale du cinquième degré, prouve du moins l'impossibilité de former une résolvante dont le degré soit inférieur à cinq.

Des substitutions circulaires.

Pour bien comprendre les développements dans lesquels nous allons entrer, il est nécessaire de se faire une idée précise de l'opération que nous avons désignée par le mot de *substitution* (*voir* onzième leçon).

(*) *Journal de l'École Polytechnique*, XXXe cahier.



Soit

$$F(a, b, c, \ldots, k, l)$$

une fonction de n lettres. Si, parmi ces n lettres, on en prend p au hasard,

$$a, b, c, \ldots, g$$

par exemple, et qu'après les avoir rangées en cercle on mette chacune d'elles à la place de celle qui la précède, on dit que l'on a fait subir à ces p lettres une permutation circulaire, et la substitution

$$\begin{pmatrix} a, & b, & c, \ldots, & g \\ b, & c, \ldots, & g, & a \end{pmatrix},$$

est dite une substitution circulaire de l'ordre p. Cela posé, on a le théorème suivant :

THÉORÈME. — *Toute substitution, si elle n'est pas circulaire, équivaut à plusieurs substitutions circulaires effectuées simultanément sur des lettres différentes.*

Supposons, en effet, que l'on fasse subir une substitution quelconque aux lettres

$$a, b, c, \ldots, f, g;$$

par cette substitution, a se trouve remplacé par une certaine lettre, c par exemple, c lui-même sera remplacé par une troisième lettre e, et, en continuant de cette manière, on tombera nécessairement sur une lettre qui se trouvera remplacée par a. Or il est évident que les lettres que l'on a ainsi rencontrées ont subi une permutation circulaire. En prenant une des lettres restantes, et opérant de la même manière, on formera un nouveau groupe de lettres qui auront subi également une permutation circulaire,

et ainsi de suite, jusqu'à ce que toutes les lettres soient épuisées.

En opérant ainsi sur la substitution

$$\begin{pmatrix} a, & b, & c, & d, & e, & f, & g, & h, & i, & j, & o \\ h, & o, & d, & f, & b, & j, & a, & g, & e, & c, & i \end{pmatrix},$$

on trouvera qu'elle équivaut aux trois substitutions circulaires suivantes :

$$\begin{pmatrix} a, & h, & g \\ h, & g, & a \end{pmatrix} \begin{pmatrix} b, & o, & i, & e \\ o, & i, & e, & b \end{pmatrix} \begin{pmatrix} c, & d, & f, & j \\ d, & f, & j, & c \end{pmatrix}.$$

Le même procédé doit aussi être employé quand on veut reconnaître si une substitution est circulaire ou non. Ainsi on trouvera que la substitution

$$\begin{pmatrix} a, & b, & c, & d, & e, & f, & g, & h, & i, & j, & o \\ g, & d, & f, & j, & a, & o, & c, & i, & b, & e, & h \end{pmatrix}$$

est circulaire, car on peut l'écrire de la manière suivante :

$$\begin{pmatrix} a, & g, & c, & f, & o, & h, & i, & b, & d, & j, & e \\ g, & c, & f, & o, & h, & i, & b, & d, & j, & e, & a \end{pmatrix}.$$

Si, après avoir effectué une permutation circulaire sur p lettres, on répète $1, 2, 3, \ldots, p-1$ fois la même permutation, on obtiendra p arrangements différents ; mais en faisant une fois de plus cette permutation, on reproduira l'arrangement primitif.

Nous désignerons par le mot *transposition* la permutation circulaire de deux lettres, c'est-à-dire l'opération qui consiste à échanger simplement ces deux lettres l'une avec l'autre, et nous indiquerons par la notation abrégée (a, b) la transposition des lettres a et b.

Il est évident que toute substitution, circulaire ou non, équivaut à une série de transpositions. Car supposons qu'il s'agisse d'opérer une substitution quelconque sur

les lettres

$$a,\ b,\ c,\ldots,\ f,\ g,$$

on amènera a à la nouvelle place qu'elle doit occuper par une transposition; cela fait, une autre transposition amènera b à la place qu'elle doit occuper, et ainsi de suite, jusqu'à ce que toutes les lettres aient pris les places qu'on veut leur donner.

Théorème de M. Cauchy.

La démonstration du théorème de M. Cauchy repose sur les quatre lemmes suivants :

LEMME Ier. — *Si une fonction de n lettres n'est pas changée par une substitution circulaire effectuée sur p lettres, elle ne changera pas non plus en répétant cette substitution un nombre quelconque de fois.*

Ce lemme est presque évident; car, soit la fonction

$$F(a,\ b,\ c,\ d,\ e,\ldots),$$

et supposons que cette fonction ne soit pas changée par la substitution circulaire du cinquième ordre

$$\begin{pmatrix} a, & b, & c, & d, & e \\ b, & c, & d, & e, & a \end{pmatrix},$$

on aura

$$F(a,\ b,\ c,\ d,\ e,\ldots) = F(b,\ c,\ d,\ e,\ a,\ldots):$$

mais cette égalité ayant lieu quelles que soient les quantités représentées par a, b, c, d, e, on aura aussi

$$\begin{aligned} F(b,\ c,\ d,\ e,\ a,\ldots) &= F(c,\ d,\ e,\ a,\ b,\ldots), \\ F(c,\ d,\ e,\ a,\ b,\ldots) &= F(d,\ e,\ a,\ b,\ c,\ldots), \\ F(d,\ e,\ a,\ b,\ c,\ldots) &= F(e,\ a,\ b,\ c,\ d,\ldots), \\ F(e,\ a,\ b,\ c,\ d,\ldots) &= F(a,\ b,\ c,\ d,\ e,\ldots); \end{aligned}$$

car chacune de ces égalités se déduit de celle qui a lieu

par hypothèse, en représentant par d'autres lettres les quantités qui étaient représentées par a, b, c, d, e.

Le même raisonnement montre que si une fonction n'est pas changée en faisant r fois de suite une permutation circulaire de p lettres, elle ne changera pas non plus en répétant $2r$ fois, $3r$ fois, etc., cette même permutation circulaire.

LEMME II. — *Réciproquement, si p est un nombre premier, et si une fonction de n lettres n'est pas changée en opérant une substitution circulaire de p lettres, un certain nombre de fois inférieur à p, cette fonction ne changera pas non plus, en faisant une seule fois la substitution circulaire.*

Désignons par

(1) 

les diverses permutations que l'on peut obtenir en appliquant p fois de suite à la fonction donnée une substitution circulaire de l'ordre p. Chacune de ces permutations se déduira de la précédente d'une manière uniforme. Si maintenant la permutation A_r donne à la fonction la même valeur que la permutation A_1, on pourra, d'après le lemme Ier, répéter un nombre quelconque de fois la substitution par laquelle on passe de la permutation A_1 à la permutation A_r. Or, pour avoir les permutations correspondantes, il suffit de joindre de r en r les sommets du polygone (1), et comme p est un nombre premier, on sait qu'on ne reviendra au point de départ qu'après avoir rencontré tous les sommets; d'où il suit que les permu-

tations

$$A_1, \; A_2, \ldots, \; A_p$$

donnent la même valeur à la fonction.

Lemme III. — *Si une fonction n'est changée par aucune substitution circulaire opérée sur p lettres, elle ne sera pas changée non plus par une substitution circulaire opérée sur trois lettres quelconques.*

Soit

$$(1) \qquad \begin{pmatrix} a, & b, & c, & d, \ldots, & k, & l \\ b, & c, & d, \ldots, & k, & l, & a \end{pmatrix}$$

une substitution circulaire d'ordre p; la substitution

$$(2) \qquad \begin{pmatrix} b, & c, & d, \ldots\ldots, & k, & l, & a \\ c, & a, & b, & d, \ldots\ldots, & k, & l \end{pmatrix}$$

sera également circulaire. En effet, en opérant, comme il a été indiqué au commencement de cette leçon, on peut écrire cette substitution de la manière suivante :

$$\begin{pmatrix} b, & c, & a, & l, \ldots, & d \\ c, & a, & l, & k, \ldots, & b \end{pmatrix}.$$

Donc, puisque, par hypothèse, la fonction qu'on considère n'est changée par aucune substitution circulaire de p lettres, on pourra, sans changer sa valeur, lui appliquer successivement les deux substitutions (1) et (2), ou, ce qui revient au même, la substitution unique

$$\begin{pmatrix} a, & b, & c, & d, \ldots, & k, & l \\ c, & a, & b, & d, \ldots, & k, & l \end{pmatrix}.$$

Mais cette dernière revient simplement à remplacer les trois lettres a, b, c, par c, a, b; la fonction ne sera donc pas changée par la substitution

$$\begin{pmatrix} a, & b, & c \\ c, & a, & b \end{pmatrix} \quad \text{ou} \quad \begin{pmatrix} a, & c, & b \\ c, & b, & a \end{pmatrix},$$

qui est circulaire, et qui doit être effectuée sur trois lettres *quelconques*.

LEMME IV. — *Si une fonction n'est changée par aucune substitution circulaire de trois lettres, elle n'a au plus que deux valeurs.*

Toute substitution circulaire de trois lettres équivaut à deux transpositions opérées successivement. Ainsi la substitution

$$\begin{pmatrix} a, b, c \\ b, c, a \end{pmatrix}$$

revient à opérer d'abord la transposition (a, b), puis ensuite la transposition (a, c), qui a une lettre commune a avec la première. Ainsi, dire qu'une fonction n'est changée par aucune substitution circulaire de trois lettres, c'est dire qu'elle n'est pas changée par deux transpositions ayant une lettre commune, opérées successivement.

Soit donc V une fonction de n lettres a, b, c, d, etc., qui n'est changée par aucune substitution circulaire de trois lettres. D'après ce qui précède, V ne changera pas en opérant successivement deux transpositions (a, b), (a, c), ayant une lettre commune. Supposons que V devienne V_1 quand on lui applique la transposition (a, b), (V_1 pouvant être égal à V), la transposition (a, c) devra changer V_1 en V, et, par suite, V en V_1; car, faire deux fois de suite une transposition, c'est ne faire aucun changement. Il résulte de là que deux transpositions (a, b), (a, c), qui ont une lettre commune, produisent le même changement sur la fonction; il en sera de même des deux transpositions (a, c), (c, d) et, par suite, des deux transpositions (a, b), (c, d) qui n'ont aucune lettre commune.

Cela posé, toute substitution équivalant à plusieurs transpositions, on voit que V n'a au plus que deux valeurs; car si une première transposition change V en V_1,

une seconde changera V_1 en V, une troisième V en V_1, et ainsi de suite ; en sorte que V n'aura que deux valeurs, et elle n'en aura même qu'une si $V = V_1$.

THÉORÈME DE M. CAUCHY. — *Si une fonction de n lettres a moins de p valeurs, p étant le plus grand nombre premier contenu dans n, elle ne peut en avoir plus de deux.*

Soient V une fonction de n lettres, p un nombre premier contenu dans n, et supposons que la fonction V ait moins de p valeurs.

Parmi les n lettres de la fonction V, prenons-en p au hasard, formons avec ces p lettres un premier arrangement A_1, puis faisons subir aux p lettres de cet arrangement une substitution circulaire, et répétons-la $p - 1$ fois; on aura en tout p arrangements que nous désignerons par

$$A_1, A_2, A_3, \ldots, A_p.$$

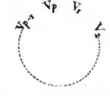
Appliquons à la fonction V les p substitutions

$$\begin{pmatrix} A_1 \\ A_1 \end{pmatrix} \begin{pmatrix} A_1 \\ A_2 \end{pmatrix} \begin{pmatrix} A_1 \\ A_3 \end{pmatrix} \cdots \begin{pmatrix} A_1 \\ A_p \end{pmatrix},$$

il en résultera p valeurs de V, que nous représenterons par

$$V_1, V_2, V_3, \ldots, V_p;$$

ou, les rangeant en cercle, par



Or, par hypothèse, la fonction V a moins de p valeurs

distinctes; il y a donc au moins deux valeurs de V égales entre elles parmi celles que nous venons d'écrire. Supposons que l'on ait

$$V_{r'+r} = V_{r'};$$

alors la fonction $V_{r'}$ ne change pas quand on fait subir aux p lettres que nous avons considérées r fois de suite une substitution circulaire, elle ne changera donc pas, p étant un nombre premier, si l'on ne fait qu'une seule fois cette substitution, et, par suite, si on la fait un nombre quelconque de fois. Mais chaque valeur de V se déduit de la précédente par une substitution circulaire des p lettres considérées; donc les p valeurs de V sont égales entre elles.

Il résulte de là que la fonction V n'est changée par aucune substitution circulaire de p lettres, donc elle ne le sera pas non plus par une substitution circulaire de trois lettres (lemme III), et, par conséquent, elle n'a que deux valeurs au plus (lemme IV).

Corollaire I. — Si n est premier, on peut prendre $p=n$, et l'on a ce théorème: *Si une fonction de n lettres, n étant premier, a moins de n valeurs, elle ne peut en avoir plus de deux.*

En particulier : *Si une fonction de cinq lettres a plus de deux valeurs, elle en a au moins cinq.*

Corollaire II. — *Toute fonction de n lettres qui a deux valeurs n'est changée par aucune substitution circulaire de trois lettres, et, par conséquent, est changée par une transposition quelconque.*

En effet, d'après le théorème précédent, une fonction qui a moins de trois valeurs n'est changée par aucune substitution circulaire de trois lettres, et, d'après le lemme IV, toutes les transpositions produisent le même changement sur la fonction; sa valeur doit donc changer par une transposition quelconque si elle n'est pas symétrique. Et,

en général, une substitution quelconque change ou ne change pas la valeur de la fonction, suivant que cette substitution équivaut à un nombre pair ou impair de transpositions.

Forme générale des fonctions qui ont deux valeurs.

On peut toujours, quel que soit n, former des fonctions de n lettres qui n'aient que deux valeurs.

Considérons, en effet, les n lettres

$$a,\ b,\ c, \ldots,\ k,\ l,$$

et désignons par ν le produit de toutes les différences obtenues, en retranchant de chacune de ces lettres successivement chacune des suivantes, on aura

$$\nu = (a-b)(a-c)\ldots(a-l)(b-c)\ldots(k-l).$$

Le carré de ν est évidemment une fonction symétrique, et, par conséquent, ν ne peut avoir que deux valeurs égales et de signes contraires. Ces deux valeurs existent effectivement; car on voit que ν se change en $-\nu$ quand on change a et b l'une dans l'autre.

On peut trouver très-facilement la forme générale des fonctions qui n'ont que deux valeurs. Désignons par V une fonction quelconque qui n'a que deux valeurs distinctes, il est aisé de voir que le produit $V\nu$ n'aura aussi que deux valeurs. Soient, en effet, V et V_1 les deux valeurs de V, ν et $-\nu$ étant celles de ν; d'après ce qui a été établi précédemment, une substitution ne changera ni V ni ν, si elle équivaut à un nombre pair de transpositions; au contraire, elle changera V en V_1 et ν en $-\nu$, si elle équivaut à un nombre impair de transpositions; d'où il suit évidemment que la fonction $V\nu$ n'a que les deux valeurs $V\nu$ et $-V_1\nu$. Si donc on fait

$$V + V_1 = A,$$
$$V\nu - V_1\nu = B,$$

A et B seront des fonctions symétriques (*voir* deuxième leçon). De ces équations, on déduit

$$V = \frac{A}{2} + \frac{B}{2v} = \frac{A}{2} + \frac{B}{2v^2}v;$$

mais $\frac{A}{2}$ et $\frac{B}{2v^2}$ sont des fonctions symétriques; on peut donc écrire plus simplement

$$V = A + Bv.$$

Telle est la forme générale des fonctions qui n'ont que deux valeurs; A et B désignent des fonctions symétriques, et v la fonction

$$(a-b)(a-c)\ldots(k-l),$$

dont les deux valeurs sont égales et de signes contraires.

VINGTIÈME LEÇON.

Sur la forme générale des fonctions de cinq lettres, qui ont cinq valeurs distinctes. — Forme des fonctions rationnelles de cinq variables qui ont cinq valeurs. — Théorème de M. Bertrand sur le nombre des valeurs que peut avoir une fonction de n lettres. — Forme générale des fonctions de n lettres qui ont n valeurs distinctes lorsque n est supérieur à 7. — Sur les fonctions de sept lettres.

Sur la forme générale des fonctions de cinq lettres qui ont cinq valeurs distinctes.

Abel a démontré, le premier (Œuvres complètes, t. I, page 19), le théorème suivant relatif aux fonctions de cinq lettres.

Théorème. — *Une fonction de cinq lettres dont le nombre des valeurs distinctes est cinq, est symétrique par rapport à quatre lettres.*

Soit V une fonction de cinq lettres

$$a,\ b,\ c,\ d,\ e,$$

ayant cinq valeurs. Si l'on y permute quatre des cinq lettres qu'elle contient, b, c, d, e, par exemple, on obtiendra un nombre de valeurs distinctes qui sera un diviseur du produit 1.2.3.4; mais, d'après l'hypothèse, ce nombre de valeurs ne peut surpasser cinq, ce sera donc l'un des quatre nombres 1, 2, 3, 4. Nous allons examiner successivement chacun de ces quatre cas.

1°. *La fonction V n'a qu'une seule valeur quand on y permute les quatre lettres b, c, d, e.*

Elle est alors symétrique par rapport à ces quatre lettres.

2°. *La fonction* V *a quatre valeurs distinctes quand on y permute les lettres* b, c, d, e.

Soient V_1, V_2, V_3, V_4, ces quatre valeurs de V, et V_5 la cinquième des valeurs que peut prendre V par les permutations des cinq lettres a, b, c, d, e.

Ainsi que nous l'avons montré précédemment (deuxième leçon), la fonction

$$V_1 + V_2 + V_3 + V_4 + V_5$$

est symétrique par rapport aux cinq lettres a, b, c, d, e. Pareillement

$$V_1 + V_2 + V_3 + V_4$$

est symétrique par rapport aux quatre lettres b, c, d, e. D'ailleurs, on a

$$V_5 = (V_1 + V_2 + V_3 + V_4 + V_5) - (V_1 + V_2 + V_3 + V_4).$$

Donc V_5 est symétrique par rapport aux lettres b, c, d, e, et, par conséquent, V est symétrique par rapport à quatre lettres.

3°. *La fonction* V *a deux valeurs quand on y permute les lettres* b, c, d, e.

Si l'on pose

$$v = (b-c)(b-d)(b-e)(c-d)(c-e)(d-e),$$

V aura, comme on l'a vu dans la dernière leçon, la forme suivante

$$V = A + Bv,$$

A et B étant des fonctions de a, b, c, d, e, symétriques par rapport à b, c, d, e.

Faisons dans V les cinq transpositions

$$(a, a), \quad (a, b), \quad (a, c), \quad (a, d), \quad (a, e).$$

et désignons par

$$A_1,\ A_2,\ A_3,\ A_4,\ A_5$$

les cinq valeurs de A, qui seront égales entre elles si A est symétrique par rapport aux cinq lettres, par

$$B_1,\ B_2,\ B_3,\ B_4,\ B_5$$

les valeurs correspondantes de B, lesquelles pourront aussi être égales entre elles, et enfin par

$$v_1,\ v_2,\ v_3,\ v_4,\ v_5$$

les valeurs correspondantes de v; on aura les dix valeurs suivantes de V,

$$\begin{array}{l} A_1 \pm B_1 v_1, \\ A_2 \pm B_2 v_2, \\ A_3 \pm B_3 v_3, \\ A_4 \pm B_4 v_4, \\ A_5 \pm B_5 v_5. \end{array}$$

Je dis que ces dix valeurs seront distinctes si A n'est pas symétrique par rapport aux lettres a, b, c, d, e, au quel cas A_1, A_2, A_3, A_4, A_5 sont différentes. En effet, si l'on avait, par exemple,

$$A_1 \pm B_1 v_1 = A_2 \pm B_2 v_2,$$

il en résulterait

$$A_1 - A_2 = \pm B_2 v_2 \mp B_1 v_1;$$

ce qui est impossible, car le premier membre est symétrique par rapport aux trois lettres c, d, e, B_1 et B_2 le sont aussi, et nous avons vu que v_2 et v_1 changent de signe par une transposition quelconque (c, d).

L'égalité précédente peut avoir lieu si A est symétrique par rapport aux cinq lettres a, b, c, d, e, auquel cas $A_1 = A_2$; mais alors il en résulte

$$(B_1 v_1)^2 = (B_2 v_2)^2.$$

Par conséquent, la fonction $(B\nu)^2$ ne change pas par la transposition (a, b); et comme cette fonction est déjà symétrique par rapport à b, c, d, e, elle l'est aussi par rapport aux cinq lettres : donc sa racine carrée $B\nu$ n'a que deux valeurs égales et de signes contraires, V n'a donc aussi que deux valeurs.

Il résulte de là qu'une fonction de cinq lettres qui a deux valeurs par les permutations de quatre lettres, en a dix ou deux seulement par les permutations des cinq lettres. Il est donc impossible qu'une fonction de cinq lettres qui a cinq valeurs en ait deux seulement par les permutations de quatre lettres.

4°. *La fonction* V *a trois valeurs quand on y permute les lettres* b, c, d, e.

Soient V_1, V_2, V_3 ces trois valeurs de V, V_4 et V_5 les deux autres valeurs que peut prendre V, par les permutations des cinq lettres a, b, c, d, e. On a

$$V_4+V_5=(V_1+V_2+V_3+V_4+V_5)-(V_1+V_2+V_3),$$

et l'on en conclut aisément que V_4+V_5 est une fonction symétrique des quatre lettres b, c, d, e. Posons

$$(1) \qquad V_4+V_5=2A;$$

$V_1 V_2 V_3 V_4 V_5$ et $V_1 V_2 V_3$ étant aussi des fonctions symétriques de b, c, d, e (deuxième leçon), il en sera de même de leur quotient $V_4 V_5$; par conséquent $(V_4-V_5)^2$ sera aussi une fonction symétrique de b, c, d, e, et la fonction

$$(2) \qquad V_4-V_5=2B$$

n'aura que deux valeurs par les permutations de ces quatre lettres. Des égalités (1) et (2), on tire

$$V_4=A+B, \quad V_5=A-B;$$

donc V_4 et V_5 n'ont que deux valeurs par les permuta-

tions des quatre lettres b, c, d, e, et, par conséquent, V aura aussi deux valeurs seulement par les permutations de quatre lettres parmi les cinq, a, b, c, d, e; et, d'après ce qu'on a vu précédemment, elle en aura dix ou deux seulement par les permutations des cinq lettres. Il est donc impossible qu'une fonction de cinq lettres qui a cinq valeurs en ait trois par les permutations de quatre de ces cinq lettres.

Ainsi une fonction de cinq lettres qui a cinq valeurs est nécessairement symétrique par rapport à quatre d'entre elles. Il est d'ailleurs évident qu'une fonction de cinq lettres symétrique par rapport à quatre d'entre elles, a effectivement cinq valeurs, et, plus généralement, qu'une fonction de n lettres symétrique par rapport à $n-1$ d'entre elles a précisément n valeurs.

Forme des fonctions rationnelles de cinq variables qui ont cinq valeurs.

Soient a, b, c, d, e cinq variables quelconques; formons l'équation du cinquième degré

$$X = x^5 + px^4 + qx^3 + rx^2 + sx + t = 0,$$

qui a a, b, c, d, e pour racines, et dont les coefficients p, q, r, s, t sont des fonctions symétriques. Soit aussi

$$V = \frac{F(a,\ b,\ c,\ d,\ e)}{f(a,\ b,\ c,\ d,\ e)}$$

une fonction rationnelle de a, b, c, d, e ayant cinq valeurs, et qui est, par conséquent, symétrique par rapport à quatre de ces cinq lettres, que nous supposerons être b, c, d, e; F et f désignent ici des fonctions entières et symétriques des racines de l'équation

$$\frac{X}{x-a} = 0,$$

qu'on pourra exprimer rationnellement par les coefficients de cette équation, c'est-à-dire en fonction de a et des fonctions symétriques p, q, etc. V est donc une fonction rationnelle de a, et peut se mettre sous la forme d'un polynôme du quatrième degré en a (*voir* deuxième leçon).

La forme la plus générale des fonctions rationnelles de cinq variables, qui ont cinq valeurs, est donc

$$V = A + Bx + Cx^2 + Dx^3 + Ex^4,$$

x désignant l'une de ces variables, et A, B, etc., des fonctions symétriques.

Corollaire. — Il résulte de là que si l'on cherchait à faire dépendre la résolution de l'équation générale du cinquième degré de celle d'une résolvante, qui fût aussi du cinquième, on retomberait forcément sur la transformation de Tschirnaüs que nous avons indiquée dans une précédente leçon.

Théorème de M. Bertrand sur le nombre de valeurs que peut avoir une fonction de n lettres.

Postulatum. — Si n est un nombre entier > 7, il y a au moins un nombre premier p compris entre $n-2$ et $\frac{n}{2}$. Cette proposition peut se vérifier à l'aide des Tables de nombres premiers pour toutes les valeurs de n inférieures à 6 000 000.

La démonstration du théorème de M. Bertrand, ainsi que celle du lemme qui va suivre, repose sur ce postulatum.

Lemme. — Soit

$$V = F(a, b, c, d, \ldots, k, l)$$

une fonction de n lettres ayant moins de n valeurs. Si p

désigne un nombre premier, compris entre $n-2$ *et* $\frac{n}{2}$, *ou égal à* $\frac{n}{2}$, *et qu'avec les* n *lettres,*

$$a, b, c, d, \ldots, k, l$$

on forme deux groupes, l'un de p, *l'autre de deux lettres, il y aura au moins un de ces deux groupes jouissant de la propriété que la fonction* V *ne sera pas changée par une permutation circulaire des lettres qui le composent.*

Soient a et b deux lettres quelconques parmi les n lettres données a, b, c, etc., on formera, en les transposant, les deux arrangements (a, b), (b, a). Considérons aussi l'un des arrangements de p lettres prises parmi les $n-2$ qui restent, faisons subir aux lettres de cet arrangement une permutation circulaire, et répétons-la $p-1$ fois; on formera, de cette façon, p arrangements; et, en combinant chacun de ces p arrangements avec les deux des lettres a et b, on aura en tout $2p$ arrangements des $p+2$ lettres, auxquels correspondront $2p$ valeurs de la fonction V. Mais, par hypothèse, V a moins de n valeurs distinctes, et $2p$ est au moins égal à n; donc, parmi les $2p$ valeurs de V, il y en a au moins deux qui sont égales entre elles. Cela posé, il convient de distinguer trois cas:

1°. Les deux valeurs égales de V correspondent à un même arrangement des p lettres et ne diffèrent que par l'ordre des deux lettres a et b. Alors on passe de l'une à l'autre des valeurs de V, par la transposition (a, b). Cette transposition ne change donc pas la valeur de V.

2°. Les deux valeurs égales de V correspondent à un même arrangement des deux lettres a et b, et à des arrangements différents des p autres lettres. Alors la fonction V n'est pas changée en répétant plusieurs fois une

permutation circulaire de ces p lettres; donc elle ne changera pas non plus en ne faisant qu'une seule fois cette permutation.

3°. Enfin, les deux valeurs de V correspondent à des arrangements qui diffèrent tant par l'ordre des deux lettres a et b que par celui des p autres lettres. Alors la fonction V n'est pas changée en répétant un certain nombre r de fois une permutation circulaire des p lettres, pourvu qu'on change en même temps a et b l'une dans l'autre. On pourra donc faire une seconde fois cette opération sans changer la valeur de V, mais alors a et b auront repris leurs places, et l'on aura seulement fait subir aux p lettres de l'autre groupe $2r$ fois une même permutation circulaire. D'où il suit, comme dans le second cas, qu'une permutation circulaire des p lettres ne changera pas la fonction. Et comme, après avoir fait plusieurs fois la permutation circulaire de ces p lettres, on peut, sans changer V, faire la transposition (a, b), cette transposition ne changera pas non plus la valeur de la fonction.

La proposition est donc démontrée.

Remarque. — La démonstration qui précède se fait, comme on voit, avec le même succès, que p soit compris entre $n-2$ et $\frac{n}{2}$, ou qu'il soit précisément égal à $\frac{n}{2}$. Mais si p est $>\frac{n}{2}$, on peut étendre un peu l'énoncé de la proposition, et dire :

Si une fonction de n lettres n'a pas plus de n valeurs, et si p désigne un nombre premier compris entre $n-2$ et $\frac{n}{2}$, en formant deux groupes, l'un de deux, l'autre de p lettres, il y aura au moins l'un de ces groupes qui jouira de la propriété que la fonction ne sera pas changée par une permutation circulaire des lettres qui le composent.

Ce nouvel énoncé ne serait pas exact si, entre $n-2$ et $\frac{n}{2}$, il n'y avait effectivement aucun nombre premier. Tel est le cas de $n=6$.

THÉORÈME DE M. BERTRAND. — *Si une fonction de n lettres, non symétrique, a moins de n valeurs, elle ne peut en avoir plus de deux.*

Supposons que la fonction

$$V = F(a, b, c, d, \ldots, k, l)$$

des n lettres a, b, c, etc., ait moins de n valeurs. Cette fonction n'étant pas symétrique, il y aura au moins deux lettres a et b dont la transposition changera sa valeur. Désignons par p un nombre premier compris entre $n-2$ et $\frac{n}{2}$, ou égal à $\frac{n}{2}$, puis parmi les $n-2$ lettres

$$c, d, \ldots, k, l,$$

prenons-en p au hasard. D'après le lemme précédent, la fonction V ne sera pas changée par une permutation circulaire de ces p lettres, puisqu'elle est changée par celle des deux lettres a et b, et que, parmi les deux groupes, l'un de deux, l'autre de p lettres, il y en a un dont la permutation circulaire ne la change pas.

Il suit de là que V, considérée comme fonction des $n-2$ lettres

$$c, d, \ldots, k, l,$$

n'est changée par aucune substitution circulaire de p lettres ; par suite, elle ne l'est pas non plus par une permutation circulaire de trois lettres, elle n'a donc au plus que deux valeurs (*voir* la leçon précédente).

Nous examinerons d'abord le cas où la fonction V est symétrique par rapport aux $n-2$ lettres c, d, ..., k, l, puis celui où elle a deux valeurs par les permutations de ces lettres.

1°. V *est symétrique par rapport aux $n-2$ lettres* $c, d, \ldots, k, l$.

Si V n'a pas précisément n valeurs, cette fonction changera par la transposition de l'une des lettres a et b avec l'une quelconque des $n-2$ autres; car autrement V serait symétrique par rapport à $n-1$ lettres, et aurait précisément n valeurs. On ne peut donc avoir

$$F(a, b, c, d, \ldots, k, l) = F(a, c, b, d, \ldots, k, l).$$

Il n'est pas possible non plus que V conserve la même valeur lorsque les deux lettres a et b sont changées en deux autres c et d, car on aurait alors

$$F(a, b, c, d, \ldots, k, l) = F(c, d, a, b, \ldots, k, l);$$

et le second membre serait symétrique par rapport à a et b, tandis que le premier ne l'est pas par hypothèse. Enfin l'égalité

$$F(a, b, c, d, \ldots, k, l) = F(b, c, a, d, \ldots, k, l)$$

est de même impossible; car le second membre est symétrique par rapport à a et d, tandis que le premier ne l'est pas.

D'où il suit que, si V n'a pas précisément n valeurs, cette fonction en aura autant qu'il y a d'arrangements de n lettres deux à deux, c'est-à-dire $n(n-1)$.

Comme, par hypothèse, la fonction V a moins de n valeurs, il est impossible qu'elle soit symétrique par rapport aux $n-2$ lettres $c, d, \ldots, k, l$.

2°. V *a deux valeurs par les permutations des $n-2$* lettres $c, d, \ldots, k, l$.

Je dis que, dans ce cas, la fonction V ne sera changée par aucune permutation circulaire de p lettres prises parmi les n

$$a, b, c, d, \ldots, k, l,$$

et, par suite, qu'elle n'aura que deux valeurs distinctes par les permutations de ces n lettres.

Remarquons d'abord que V n'ayant que deux valeurs, par les permutations des $n-2$ lettres $c, d, \ldots, k, l$ change par une transposition quelconque de deux de ces lettres, et n'est pas changée par une permutation circulaire opérée sur p de ces $n-2$ lettres. Supposons, en second lieu, qu'on prenne p lettres parmi les n lettres a, b, etc., et que parmi ces p lettres se trouvent a et b ou au moins l'une d'elles, il y aura au plus dans ce groupe $p-1$ lettres prises parmi $c, d, \ldots, k, l$; et comme p est $< n-2$, il restera au moins deux de ces dernières lettres qui ne feront pas partie du groupe de p lettres. Or la transposition de ces deux-là change la valeur de la fonction; donc, d'après le lemme précédent, la permutation circulaire des p lettres ne la changera pas.

La fonction V n'étant changée par aucune permutation circulaire de p lettres, ne le sera pas non plus par une permutation circulaire de trois lettres, et, par conséquent, elle n'aura que deux valeurs, ainsi que nous l'avons vu dans la dernière leçon.

On voit donc que si entre $n-2$ et $\frac{n}{2}$ il y a un nombre premier, ou si $\frac{n}{2}$ est un nombre premier, une fonction de n lettres qui a moins de n valeurs ne peut en avoir que deux au plus.

En particulier, comme $\frac{6}{2}$ est un nombre premier, on a ce théorème démontré depuis longtemps par M. Cauchy:

Une fonction de six lettres, qui a moins de six valeurs, ne peut en avoir plus de deux.

Sur la forme des fonctions de n lettres qui ont n valeurs.

Soit

$$V = F(a, b, c, d, \ldots, k, l)$$

une fonction de n lettres $a, b, c, \ldots, k, l$, qui a précisément n valeurs, et supposons que la transposition (a, b) change la valeur de cette fonction ; on fera voir, comme précédemment, que la fonction V ne peut avoir que deux valeurs au plus par les permutations des $n-2$ lettres c, $d, \ldots, k, l$, pourvu qu'il existe un nombre premier compris entre $n-2$ et $\frac{n}{2}$: alors la fonction V doit être symétrique par rapport aux $n-2$ lettres $c, d, \ldots, k, l$, car, s'il en était autrement, on a vu qu'elle n'aurait que deux valeurs. Je dis même qu'elle doit être symétrique par rapport à $n-1$ lettres, car autrement elle aurait $n(n-1)$ valeurs, comme nous l'avons fait voir tout à l'heure ; d'où il résulte que, s'il existe un nombre premier compris entre $n-2$ et $\frac{n}{2}$, on a ce théorème, déjà démontré pour $n=5$.

Théorème. — *Une fonction de n lettres qui a n valeurs est symétrique par rapport à n — 1 lettres.*

Remarque. — La démonstration ne s'applique pas aux fonctions de six lettres, et il est très-remarquable que le théorème n'ait pas lieu dans ce cas. Il y a, en effet, des fonctions de six lettres qui ont six valeurs, sans être symétriques par rapport à cinq lettres.

Sur les fonctions de sept lettres.

La démonstration que M. Bertrand a donnée de son théorème ne s'applique pas aux fonctions de sept lettres, parce qu'entre $7-2$ et $\frac{7}{2}$ il n'y a aucun nombre premier ;

mais, comme 7 est un nombre premier, le cas des fonctions de sept lettres est compris dans le théorème de M. Cauchy.

Quant aux fonctions de sept lettres qui ont précisément sept valeurs, il est très-facile de démontrer qu'elles sont symétriques par rapport à six lettres.

Soit, en effet,

$$V = F(a, b, c, d, e, f, g)$$

une fonction de sept lettres ayant sept valeurs; le nombre des valeurs que prend V, par les permutations de six lettres, b, c, d, e, f, g par exemple, doit être un diviseur de $1.2.3.4.5.6$; et comme ce nombre est au plus égal à 7, ce sera nécessairement l'un des nombres 1, 2, 3, 4, 5 ou 6. D'ailleurs une fonction de six lettres qui a moins de six valeurs n'en a au plus que deux; donc notre fonction V ne peut avoir que une, deux ou six valeurs par les permutations des six lettres b, c, d, e, f, g. Examinons ces trois cas :

1°. Si V n'a qu'une valeur par les permutations des lettres b, c, d, e, f, g, elle est symétrique par rapport à ces lettres.

2°. Si V a six valeurs $V_1, V_2, V_3, V_4, V_5, V_6$ par les permutations des six lettres, et que V_7 soit la septième valeur de V, on prouvera, comme nous l'avons fait pour les fonctions de cinq lettres, que V_7 est symétrique par rapport aux six lettres b, c, d, e, f, g. Par suite, V est symétrique par rapport à six lettres.

3°. Si V a deux valeurs par les permutations des six lettres b, c, d, e, f, g, en posant

$$v = (b - c)(b - d) \ldots (f - g),$$

V aura la forme

$$V = A + Bv,$$

A et B désignant des fonctions de a, b, c, d, e, f, g symétriques par rapport aux six dernières, et l'on fera voir, par un raisonnement identique à celui que nous avons employé pour les fonctions de cinq lettres, que V aurait alors quatorze valeurs ou deux seulement.

D'où il suit, comme nous l'avions annoncé, qu'une fonction de sept lettres, qui a sept valeurs, est symétrique par rapport à six lettres.

VINGT ET UNIÈME LEÇON.

Des fonctions algébriques. — Des fonctions entières. — Des fonctions rationnelles. — Classification des fonctions algébriques non rationnelles. — Forme générale des fonctions algébriques.

Des fonctions algébriques.

Les considérations développées dans la dix-huitième leçon et les suivantes donnent lieu de penser, sans toutefois le démontrer d'une manière rigoureuse, qu'il est impossible de résoudre algébriquement les équations générales de degré supérieur au quatrième. Abel est parvenu à démontrer cette impossibilité, par une méthode qui a été simplifiée ensuite par Wantzel dans quelques-unes de ses parties.

Résoudre une équation algébriquement, c'est former une fonction algébrique des coefficients qui, substituée à l'inconnue, satisfasse identiquement à l'équation; la première chose à faire, pour reconnaître si une équation est soluble ou non algébriquement, est donc d'étudier la forme générale des fonctions algébriques. C'est cette étude que nous allons faire ici, et nous démontrerons, dans la prochaine leçon, l'impossibilité de résoudre algébriquement les équations générales de degré supérieur au quatrième.

Soient

$$x_1,\ x_2,\ x_3, \ldots,\ x_k,$$

k quantités quelconques indépendantes, et v une fonction de ces quantités; v sera une *fonction algébrique*, si l'on

peut l'exprimer en x_1, x_2, x_3, etc., à l'aide des opérations suivantes, effectuées un nombre fini de fois : 1° l'addition ou la soustraction; 2° la multiplication; 3° la division; 4° l'extraction des racines d'indices premiers. Nous ne comptons pas l'élévation aux puissances entières et l'extraction des racines de degrés composés, car ces opérations sont évidemment comprises dans les quatre que nous avons mentionnées

Des fonctions entières.

Lorsque la fonction v peut se former par les deux premières des quatre opérations mentionnées ci-dessus, elle est dite rationnelle et entière ou simplement entière.

Désignons par

$$f(x_1, x_2, x_3, \ldots)$$

une fonction qui peut être exprimée par une somme d'un nombre limité de termes de la forme

$$\mathrm{A}x_1^{m_1}\ x_2^{m_2}\ldots$$

A étant une constante, et m_1, m_2, etc., des exposants entiers et positifs. L'opération désignée par f fournit une fonction entière, conformément à la définition précédente; et l'on peut généralement considérer toutes les fonctions entières comme obtenues en répétant cette opération un nombre limité de fois. Soient v_1, v_2, etc., plusieurs fonctions de x_1, x_2, etc., de la même forme que f, la fonction

$$f(v_1, v_2, \ldots)$$

sera évidemment de la même forme. D'ailleurs $f(v_1, v_2, \ldots)$ est l'expression des fonctions obtenues en répétant deux fois l'opération $f(x_1, x_2, \ldots)$; d'où il suit qu'on trouvera toujours un résultat de même forme, en répétant cette

même opération autant de fois que l'on voudra, et que toute fonction entière de x_1, x_2, etc., peut être exprimée par une somme de termes de la forme

$$A x_1^{m_1} x_2^{m_2} \ldots.$$

Des fonctions rationnelles.

Une fonction v des quantités x_1, x_2, x_3, etc., est dite rationnelle lorsqu'elle peut être exprimée par les trois premières des quatre opérations algébriques ci-dessus désignées.

Soient

$$f(x_1,\ x_2,\ x_3,\ldots), \qquad F(x_1,\ x_2,\ x_3,\ldots)$$

deux fonctions entières, le quotient de ces fonctions

$$\frac{f(x_1,\ x_2,\ldots)}{F(x_1,\ x_2,\ldots)}$$

sera évidemment un cas particulier des fonctions rationnelles non entières, et l'on peut considérer toute fonction rationnelle comme obtenue en répétant plusieurs fois l'opération précédente; mais en désignant par v_1, v_2, etc., plusieurs fonctions de la forme $\frac{f(x_1,\ x_2,\ldots)}{F(x_1,\ x_2,\ldots)}$, il est évident que la fonction

$$\frac{f(v_1,\ v_2,\ldots)}{F(v_1,\ v_2,\ldots)}$$

peut être réduite à la même forme; d'où il suit que toute fonction rationnelle se réduira à la forme

$$\frac{f(x_1,\ x_2,\ldots)}{F(x_1,\ x_2,\ldots)},$$

f et F désignant des fonctions entières.

Classification des fonctions algébriques non rationnelles.

Soit

$$f(x_1,\ x_2, \ldots)$$

une fonction rationnelle quelconque; il est évident que toute fonction algébrique s'obtiendra en combinant l'opération désignée par f avec l'opération désignée par $\sqrt[m]{}$, m étant un nombre premier. Si donc p_1, p_2 désignent des fonctions rationnelles de x_1, x_2, etc., n_1, n_2, etc., des nombres premiers, et qu'on fasse

$$p' = f\left(x_1,\ x_2, \ldots,\ \sqrt[n_1]{p_1},\ \sqrt[n_2]{p_2}, \ldots\right),$$

p' sera la forme des fonctions algébriques dans lesquelles l'opération désignée par $\sqrt{}$ ne porte que sur des fonctions rationnelles. Nous appellerons, avec Abel, *fonctions algébriques du premier ordre* les fonctions de la forme p'.

Soient p'_1, p'_2, etc., des fonctions algébriques du premier ordre, n'_1, n'_2, etc., des nombres premiers; et posons

$$p'' = f\left(x_1,\ x_2, \ldots,\ \sqrt[n_1]{p_1},\ \sqrt[n_2]{p_2}, \ldots,\ \sqrt[n'_1]{p'_1},\ \sqrt[n'_2]{p'_2}, \ldots\right),$$

p'' sera la forme générale des fonctions algébriques dans lesquelles l'opération désignée par $\sqrt[m]{}$ ne porte que sur des fonctions rationnelles ou sur des fonctions algébriques du premier ordre. Nous appellerons *fonctions algébriques du deuxième ordre* les fonctions de la forme p''.

De même si p''_1, p''_2, etc., désignent des fonctions algébriques du deuxième ordre, n''_1, n''_2, etc., des nombres premiers, et qu'on fasse

$$p''' = f\left(x_1,\ x_2, \ldots,\ \sqrt[n_1]{p_1}, \ldots,\ \sqrt[n'_1]{p'_1}, \ldots,\ \sqrt[n''_1]{p''_1}, \ldots\right),$$

p''' sera la forme des fonctions algébriques, où l'opération désignée par $\sqrt[m]{}$ ne porte que sur des fonctions rationnelles et sur des fonctions des deux premiers ordres. Les fonctions de la forme p''' seront les fonctions algébriques du troisième ordre.

En continuant ainsi, on formera des fonctions algébriques du quatrième, cinquième, etc., $\mu^{\text{ième}}$ ordre, et il est évident que l'expression générale des fonctions du $\mu^{\text{ième}}$ ordre sera l'expression générale des fonctions algébriques.

Il suit de là qu'en désignant par v une fonction algébrique du $\mu^{\text{ième}}$ ordre, v aura la forme

$$v = f\left(r_1,\ r_2, \ldots,\ \sqrt[n_1]{p_1},\ \sqrt[n_2]{p_2}, \ldots\right),$$

où f désigne toujours une fonction rationnelle, p_1, p_2, etc., des fonctions de l'ordre $\mu - 1$, n_1, n_2, etc., des nombres premiers, et r_1, r_2, etc., des fonctions de l'ordre $\mu - 1$ ou d'ordres moins élevés.

On peut évidemment supposer qu'aucun des radicaux $\sqrt[n_1]{p_1}$, $\sqrt[n_2]{p_2}$, etc., ne soit exprimable rationnellement en fonctions des autres radicaux et des quantités r_1, r_2, etc. Si, en effet, $\sqrt[n_1]{p_1}$ était dans ce cas, en portant sa valeur dans l'expression de v, on aurait une valeur de v

$$v = f\left(r_1,\ r_2, \ldots,\ \sqrt[n_2]{p_2}, \ldots\right)$$

de la même forme que la précédente, mais plus simple, puisqu'elle contiendrait le radical $\sqrt[n_1]{p_1}$ de moins. Si de même l'un des radicaux qui restent pouvait s'exprimer en fonction rationnelle des autres radicaux et des quantités r_1, r_2, etc., on pourrait chasser ce radical de l'expression de v, qui conserverait d'ailleurs la même forme;

et si l'on pouvait ainsi continuer jusqu'à ce qu'on eût éliminé tous les radicaux $\sqrt[n_1]{p_1}$, $\sqrt[n_2]{p_2}$, etc., la fonction v serait réduite à l'ordre $\mu - 1$.

Si donc la fonction v est effectivement du $\mu^{ième}$ ordre, on peut supposer que les radicaux $\sqrt[n_1]{p_1}$, $\sqrt[n_2]{p_2}$, etc., aient été réduits au plus petit nombre possible, et qu'il soit impossible d'exprimer l'un de ces radicaux en fonction rationnelle des autres et de fonctions algébriques d'ordre inférieur. Et si m désigne alors le nombre de ces radicaux qui affectent des fonctions algébriques d'ordre $\mu - 1$, nous dirons que la fonction v d'ordre μ est du *degré m*.

D'après cette définition, une fonction d'ordre μ et de degré 0 n'est autre qu'une fonction d'ordre $\mu - 1$, et une fonction d'ordre 0 est une fonction rationnelle.

Il résulte de là que si v désigne une fonction algébrique d'ordre μ et de degré m, on aura généralement

$$v = f\left(r_1,\ r_2, \ldots,\ \sqrt[n]{p}\right),$$

f désignant une fonction rationnelle, p une fonction algébrique d'ordre $\mu - 1$, n un nombre premier, et r_1, r_2, etc., des fonctions d'ordre μ, mais de degré $m - 1$. En outre, d'après ce qui précède, on peut toujours supposer qu'il soit impossible d'exprimer $\sqrt[n]{p}$ en fonction rationnelle de r_1, r_2, etc.

Forme générale des fonctions algébriques.

Dans l'expression précédente de v, f désigne une fonction rationnelle des quantités r_1, r_2, etc., et $\sqrt[n]{p}$; mais toute fonction rationnelle de plusieurs quantités peut être représentée par le quotient de deux fonctions en-

tières, nous pouvons donc poser

$$v = \frac{\varphi\left(r_1, r_2, \ldots, \sqrt[n]{p}\right)}{\psi\left(r_1, r_2, \ldots, \sqrt[n]{p}\right)},$$

φ et ψ désignant des fonctions entières, et si l'on ordonne φ et ψ par rapport aux puissances de $\sqrt[n]{p}$ ou $p^{\frac{1}{n}}$, on aura pour v une valeur de la forme

$$v = \frac{s_0 + s_1 p^{\frac{1}{n}} + s_2 p^{\frac{2}{n}} + \ldots + s_\nu p^{\frac{\nu}{n}}}{t_0 + t_1 p^{\frac{1}{n}} + t_2 p^{\frac{2}{n}} + \ldots + t_{\nu'} p^{\frac{\nu'}{n}}} = \frac{S}{T},$$

où $s_0, s_1, \ldots, s_\nu$ et $t_0, t_1, \ldots, t_{\nu'}$, sont des fonctions entières de r_1, r_2, etc.

Soit α une racine imaginaire de l'équation

$$\alpha^n = 1;$$

désignons par

$$T_1, T_2, \ldots, T_{n-1}$$

les $n-1$ valeurs qu'on obtient en remplaçant dans T, $p^{\frac{1}{n}}$ successivement par

$$\alpha p^{\frac{1}{n}}, \quad \alpha^2 p^{\frac{1}{n}}, \quad \alpha^3 p^{\frac{1}{n}}, \ldots, \alpha^{n-1} p^{\frac{1}{n}},$$

et multiplions par $T_1 T_2 \ldots T_{n-1}$ les deux termes de la valeur de v, on aura

$$v = \frac{ST_1T_2\ldots T_{n-1}}{TT_1T_2\ldots T_{n-1}}.$$

Le produit $T_1 T_2 \ldots T_{n-1}$ peut évidemment s'exprimer en fonction entière de p et des quantités r_1, r_2, etc.; il est donc une fonction algébrique d'ordre μ et de degré $m-1$

au plus, que nous désignerons par u. Pareillement, le produit $ST_1 T_2 \ldots T_{n-1}$ est une fonction entière de r_1, r_2, etc., et $\sqrt[n]{p}$; nous représenterons sa valeur par

$$u_0 + u_1 p^{\frac{1}{n}} + u_2 p^{\frac{2}{n}} + \ldots + u_i p^{\frac{i}{n}},$$

et l'on aura

$$v = \frac{u_0 + u_1 p^{\frac{1}{n}} + u_2 p^{\frac{2}{n}} + \ldots + u_i p^{\frac{i}{n}}}{u},$$

ou simplement

$$v = q_0 + q_1 p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots + q_i p^{\frac{i}{n}},$$

en mettant q_0, q_1, etc., au lieu de $\frac{u_0}{u}$, $\frac{u_1}{u}$, etc. q_0, q_1, etc., désignent ici des fonctions rationnelles de r_1, r_2, etc., et p.

On peut chasser de l'expression précédente de v les puissances de $p^{\frac{1}{n}}$ supérieures à la $(n-1)^{\text{ième}}$. Si, en effet, j désigne un nombre qui, divisé par n, donne le quotient g et le reste h, on a

$$p^{\frac{j}{n}} = p^g \cdot p^{\frac{h}{n}},$$

et, en se servant de cette formule, on pourra mettre v sous la forme

$$(1) \qquad v = q_0 + q_1 p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots + q_{n-1} p^{\frac{n-1}{n}},$$

q_0, q_1, q_2, ..., q_{n-1} étant toujours des fonctions rationnelles de p, r_1, r_2, etc., et, par conséquent, des fonctions algébriques d'ordre μ et de degré $m-1$ au plus, telles, en outre, qu'il soit impossible d'exprimer rationnellement $p^{\frac{1}{n}}$ en fonction des quantités dont elles dépendent.

Dans l'expression (1) de v, on peut supposer

$$q_1 = 1.$$

Pour le démontrer, supposons d'abord que q_1 ne soit pas nul, et posons

$$p_1 = pq_1^n;$$

d'où

$$p = \frac{p_1}{q_1^n} \quad \text{et} \quad p^{\frac{1}{n}} = \frac{p_1^{\frac{1}{n}}}{q_1};$$

l'expression de v devient

$$v = q_0 + p_1^{\frac{1}{n}} + \frac{q_2}{q_1^2} p^{\frac{2}{n}} + \ldots + \frac{q_{n-1}}{q_1^{n-1}} p^{\frac{n-1}{n}},$$

ou plus simplement

$$(2) \qquad v = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots + q_{n-1} p^{\frac{n-1}{n}},$$

en écrivant p au lieu de p_1; q_2, q_3, etc., au lieu de $\frac{q_2}{q_1^2}$, $\frac{q_3}{q_1^3}$, etc.

Dans cette nouvelle expression (2) de v qui se déduit de (1) en faisant $q_1 = 1$, les quantités q_0, q_2, etc., désignent toujours des fonctions algébriques d'ordre μ et de degré $m-1$.

Supposons maintenant que dans l'expression (1) de v on ait $q_1 = 0$; désignons par q_k l'une des quantités q_1, q_2, etc., qui n'est pas nulle, et posons

$$p_1 = q_k^n p^k,$$

d'où

$$p_1^{\frac{\alpha}{n}} = q_k^{\alpha} p^{\frac{k\alpha}{n}}.$$

n étant premier et k moindre que n, on peut toujours

trouver deux entiers α et β tels, que

$$k\alpha - n\beta = \lambda,$$

λ étant un nombre entier quelconque donné; alors on aura

$$p_1^{\frac{\alpha}{n}} = q_k^{\alpha} p^{\beta} p^{\frac{\lambda}{n}};$$

d'où

$$p^{\frac{\lambda}{n}} = q_k^{-\alpha} p^{-\beta} p_1^{\frac{\alpha}{n}}.$$

On a, en particulier et par hypothèse,

$$p^{\frac{k}{n}} = \frac{p_1^{\frac{1}{n}}}{q_k};$$

à l'aide des deux formules précédentes, on substituera aux puissances de $p^{\frac{1}{n}}$ dans la valeur (1) de v, celles de $p_1^{\frac{1}{n}}$, et, après cette substitution, il est évident que la forme de v n'aura pas changé, mais que le coefficient de $p_1^{\frac{1}{n}}$ sera l'unité; car, dans l'expression primitive de v, $p^{\frac{k}{n}}$ a pour coefficient q_k.

Conclusion. — *Il résulte de ce qui précède que toute fonction algébrique d'ordre μ et de degré m peut être mise sous la forme*

$$v = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots + q_{n-1} p^{\frac{n-1}{n}},$$

où n est un nombre premier, q_0, q_2, etc., des fonctions algébriques d'ordre μ, mais de degré $m-1$, et p une fonction d'ordre $\mu - 1$, dont la racine $n^{ième}$ ne peut être exprimée rationnellement par les quantités q_0, q_2, etc.

VINGT-DEUXIÈME LEÇON.

Propriétés des fonctions algébriques qui satisfont à une équation donnée. — Démonstration de l'impossibilité de résoudre algébriquement les équations générales de degré supérieur au quatrième.

Propriétés des fonctions algébriques qui satisfont à une équation donnée.

Si l'on considère un polynôme entier et rationnel

$$x^m + a_1 x^{m-1} + a_2 x^{m-2} + \ldots,$$

dont les coefficients a_1, a_2, etc., sont des fonctions rationnelles de quantités quelconques, qu'on regarde comme connues, tout diviseur de ce polynôme qui a pour coefficients des fonctions rationnelles des quantités connues, est appelé un *diviseur commensurable*.

On nomme *équation irréductible* toute équation dont le premier membre n'admet aucun diviseur commensurable.

L'équation générale de degré quelconque, dont les coefficients sont indéterminés, est nécessairement irréductible.

Cela posé, soit une équation de degré m

$$(1) \quad x^m + a_1 x^{m-1} + a_2 x^{m-2} + \ldots + a_{m-1} x + a_m = 0,$$

dont les coefficients sont considérés comme des fonctions rationnelles de quantités connues, et supposons qu'elle soit résoluble algébriquement.

D'après la classification des fonctions algébriques établie dans la leçon précédente, si la racine x est une fonction algébrique d'ordre μ des quantités connues, on pourra poser

$$(2)\qquad x = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots + q_{n-1} p^{\frac{n-1}{n}}.$$

n est un nombre premier, p désigne une fonction d'ordre $\mu - 1$; q_0, q_2, etc., peuvent être de l'ordre μ, mais sont d'un degré moindre que celui de x. Enfin, on peut supposer qu'il soit impossible d'exprimer $p^{\frac{1}{n}}$ en fonction rationnelle de p, q_0, q_1, etc.

En substituant cette expression (2) de x dans l'équation (1), on aura un résultat qui pourra évidemment se réduire à la forme

$$(3)\qquad r_0 + r_1 p^{\frac{1}{n}} + r_2 p^{\frac{2}{n}} + \ldots + r_{n-1} p^{\frac{n-1}{n}} = 0,$$

où $r_0, r_1, r_2, \ldots, r_{n-1}$ désignent des fonctions rationnelles des quantités $p, q_0, q_2, \ldots, q_{n-1}$. Or je dis que l'équation (3) exige que l'on ait en même temps

$$r_0 = 0,\quad r_1 = 0,\quad r_2 = 0, \ldots,\quad r_{n-1} = 0.$$

En effet, dans le cas contraire, les deux équations

$$z^n - p = 0,$$
$$r_0 + r_1 z + r_2 z^2 + \ldots + r_{n-1} z^{n-1} = 0$$

auraient une ou plusieurs racines communes. Soit k le nombre de ces racines, on pourrait former une équation de degré k ayant pour racines ces k racines communes, pour coefficients des fonctions rationnelles de p, q_0, $q_2, \ldots, q_{n-1}$. Soit

$$s_0 + s_1 z + s_2 z^2 + \ldots + s_k z^k = 0$$

cette équation, et désignons par

$$t_0 + t_1 z + t_2 z^2 + \ldots + t_i z^i$$

un diviseur irréductible de son premier membre, dont les coefficients $t_0, t_1, \ldots, t_i$ soient des fonctions rationnelles de $p, q_0, q_2, \ldots, q_{n-1}$. L'équation

$$(4) \qquad t_0 + t_1 z + t_2 z^2 + \ldots + t_i z^i = 0$$

a toutes ses racines communes avec

$$(5) \qquad z^n - p = 0;$$

d'ailleurs son degré i est au moins égal à 2, car, autrement, on pourrait exprimer z ou $p^{\frac{1}{n}}$ en fonction rationnelle de $p, q_0, q_2, \ldots, q_{n-1}$. Si donc z désigne une racine quelconque de l'équation (4), cette équation aura au moins une autre racine de la forme αz, α étant une racine de l'équation

$$\alpha^n = 1;$$

l'équation (4) aura donc une racine commune avec

$$(6) \qquad t_0 + t_1 \alpha z + t_2 \alpha^2 z^2 + \ldots + t_i \alpha^i z^i = 0,$$

et, par conséquent, avec l'équation

$$(7) \quad (1 - \alpha^i) t_0 + (\alpha - \alpha^i) t_1 z + \ldots + (\alpha^{i-1} - \alpha^i) t_{i-1} z^{i-1} = 0,$$

que l'on obtient en retranchant de l'équation (6) l'équation (4) multipliée par α^i. Mais l'équation (4) est supposée irréductible, il est donc impossible qu'elle ait une racine commune avec l'équation (7), qui est de degré inférieur au sien. D'où il suit qu'on a nécessairement

$$r_0 = 0, \quad r_1 = 0, \ldots, r_{n-1} = 0.$$

Les équations précédentes ayant lieu, l'expression (2) de x satisfera encore à la proposée (1), en remplaçant $p^{\frac{1}{n}}$

par chacune des n valeurs

$$p^{\frac{1}{n}},\quad \alpha p^{\frac{1}{n}},\quad 6p^{\frac{1}{n}},\ldots,\omega p^{\frac{1}{n}},$$

où $1, \alpha, 6, \ldots, \omega$ désignent les racines $n^{ièmes}$ de l'unité. On aura ainsi n racines de l'équation (1), que nous représenterons par

$$x_1,\quad x_2,\ldots,x_n,$$

et dont les valeurs seront

$$(8)\quad \begin{cases} x_1 = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots\ldots\ldots + q_{n-1} p^{\frac{n-1}{n}}, \\ x_2 = q_0 + \alpha p^{\frac{1}{n}} + \alpha^2 q_2 p^{\frac{2}{n}} + \ldots + \alpha^{n-1} q_{n-1} p^{\frac{n-1}{n}}, \\ x_3 = q_0 + 6 p^{\frac{1}{n}} + 6^2 q_2 p^{\frac{2}{n}} + \ldots + 6^{n-1} q_{n-1} p^{\frac{n-1}{n}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n = q_0 + \omega p^{\frac{1}{n}} + \omega^2 q_2 p^{\frac{2}{n}} + \ldots + \omega^{n-1} q_{n-1} p^{\frac{n-1}{n}}; \end{cases}$$

on voit que ces racines sont différentes, car, si deux d'entre elles étaient égales, on aurait une équation de cette forme

$$(\alpha - 6) q_0 + (\alpha - 6) p^{\frac{1}{n}} + (\alpha^2 - 6^2) q_2 p^{\frac{2}{n}} + \ldots = 0,$$

qui conduirait aux équations contradictoires

$$(\alpha - 6) q_0 = 0,\quad (\alpha - 6) = 0, \ldots.$$

Au surplus, cette remarque n'est pas indispensable pour ce qui va suivre.

En ajoutant les équations (8), en les ajoutant ensuite après les avoir respectivement multipliées par

$$1,\quad \alpha^{n-1},\quad 6^{n-1},\ldots,\omega^{n-1},$$

puis par

$$1,\quad \alpha^{n-2},\quad 6^{n-2},\ldots,\omega^{n-2}, \text{etc.},$$

on obtient les suivantes :

$$q_0 = \frac{1}{n}(x_1 + x_2 + x_3 + \ldots\ldots + x_n),$$

$$p^{\frac{1}{n}} = \frac{1}{n}(x_1 + \alpha^{n-1} x_2 + \ldots + \omega^{n-1} x_n),$$

$$q_2 p^{\frac{2}{n}} = \frac{1}{n}(x_1 + \alpha^{n-2} x_2 + \ldots + \omega^{n-2} x_n),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$q_{n-1} p^{\frac{n-1}{n}} = \frac{1}{n}(x_1 + \alpha x_2 + \ldots\ldots\ldots + \omega x_n).$$

Il résulte de là que les quantités

$$p^{\frac{1}{n}}, \quad q_0, \quad q_2, \ldots, q_{n-1}$$

sont des fonctions rationnelles des racines de l'équation (1). On a, en effet, généralement

$$q_\rho = n^{\rho-1} \frac{x_1 + \alpha^{n-\rho} x_2 + \beta^{n-\rho} x_3 + \ldots + \omega^{n-\rho} x_n}{(x_1 + \alpha^{n-1} x_2 + \beta^{n-1} x_3 + \ldots + \omega^{n-1} x_n)^\rho}.$$

Désignons maintenant par y l'une quelconque des quantités $p^{\frac{1}{n}}$, q_0, $q_2, \ldots, q^{n-1}$, et soit

$$(9) \qquad y = s_0 + v^{\frac{1}{r}} + s_2 v^{\frac{2}{r}} + \ldots + s_{r-1} v^{\frac{r-1}{r}},$$

s_0, s_2, etc., étant des fonctions qui peuvent être du même ordre que y, mais qui sont de degré inférieur. On a, par ce qui précède,

$$y = \varphi(x_1, x_2, \ldots, x_m),$$

φ désignant une fonction rationnelle, et $x_1, x_2, \ldots, x_m$ les m racines de l'équation (1), lesquelles peuvent ne pas entrer toutes dans la fonction φ. Soit m' le nombre de valeurs que prend la fonction φ quand on y permute les

racines x_1, x_2, etc.; on pourra former une équation du degré m' dont les coefficients seront exprimés rationnellement par ceux de l'équation (1), et dont les racines

$$y_1, \ y_2, \ldots, \ y_{m'}$$

seront les m' valeurs de la fonction φ. Et comme la valeur (9) de y doit satisfaire à cette équation, on en conclura, comme précédemment, que les quantités

$$v, \ s_0, \ s_2, \ldots, \ s_{r-1}$$

sont des fonctions rationnelles de y_1, $y_2, \ldots, y_{m'}$, et, par conséquent, aussi de x_1, $x_2, \ldots, x_m$.

Comme on peut continuer indéfiniment ce raisonnement, on conclut de ce qui précède, que

Si une équation est résoluble algébriquement, on peut donner à la racine une forme telle, que toutes les fonctions algébriques dont elle est composée soient des fonctions rationnelles des racines de l'équation proposée.

Démonstration de l'impossibilité de résoudre algébriquement les équations générales de degré supérieur au quatrième.

Les propriétés des racines d'une équation résoluble algébriquement, que nous venons de démontrer, ont lieu dans tous les cas, soit qu'il s'agisse d'une équation dont les coefficients ont des valeurs déterminées, soit que l'on considère ces coefficients comme indéterminés, et, par suite, les racines de l'équation comme étant des quantités quelconques, n'ayant entre elles aucune dépendance.

Nous plaçant maintenant à ce dernier point de vue, nous allons démontrer qu'il est impossible de résoudre algébriquement les équations générales de degré supérieur au quatrième.

Ce théorème a été démontré, pour la première fois, par Abel; mais je présenterai ici la démonstration très-remarquable de Wantzel. On verra, dans cette reproduction exacte, un hommage mérité à la mémoire d'un géomètre que la mort a frappé dans toute la force de son talent. Je supprimerai pourtant quelques détails, inutiles ici, après les développements que j'ai donnés sur le nombre de valeurs qu'une fonction peut acquérir (*).

Soit

$$f(x) = 0$$

une équation de degré m dont les coefficients sont indéterminés, et désignons par

$$x_1, x_2, \ldots, x_m$$

ses m racines, que nous supposons exprimables algébriquement en fonction de ses coefficients.

« Si l'équation $f(x) = 0$ est satisfaite par la valeur x_1 » de x, quels que soient ses coefficients, on doit reproduire identiquement x_1, en substituant dans son expression la fonction rationnelle correspondante à chaque radical, puisque les racines de l'équation sont alors entièrement arbitraires. De même, toute relation entre les racines devra être identique, et ne cessera pas d'exister, si l'on y remplace ces racines les unes par les autres, d'une manière quelconque.

» Désignons par y le premier radical qui entre dans la valeur de x_1, en suivant l'ordre du calcul, et soit

$$y^n = p;$$

» p dépendra immédiatement des coefficients de $f(x) = 0$, » et s'exprimera par une fonction symétrique des racines

(*) Les guillemets indiquent tout ce qui est emprunté littéralement au Mémoire de Wantzel.

» $F(x_1, x_2, x_3, \ldots)$; y sera une fonction rationnelle
» $\varphi(x_1, x_2, x_3, \ldots)$ des mêmes racines.

» Comme la fonction φ n'est pas symétrique, sans quoi
» la racine $n^{ième}$ de p s'extrairait exactement, elle doit
» changer lorsqu'on permute deux racines, x_1, x_2, par
» exemple; mais la relation

$$\varphi^n = F$$

» sera toujours satisfaite. D'ailleurs la fonction F étant
» invariable par cette permutation, les valeurs de φ sont
» des racines de l'équation $y^n = F$, et l'on a

$$\varphi(x_2, x_1, x_3, \ldots) = \alpha\varphi(x_1, x_2, x_3, \ldots),$$

» α étant une racine $n^{ième}$ de l'unité.

» Si l'on remplace de part et d'autre x_1 par x_2, et ré-
» ciproquement, il vient

$$\varphi(x_1, x_2, x_3, \ldots) = \alpha\varphi(x_2, x_1, x_3, \ldots);$$

» d'où, en multipliant par ordre,

$$\alpha^2 = 1.$$

» Ce résultat prouve que le nombre n, supposé pre-
» mier, est nécessairement égal à 2; *donc le premier*
» *radical qui se présente dans la valeur de l'inconnue*
» *doit être du second degré*. C'est ce qui arrive, en effet,
» pour les équations qu'on sait résoudre. »

La fonction φ, n'ayant que deux valeurs, change par une transposition quelconque, et ne sera pas changée (*voir* dix-neuvième leçon) par une permutation circulaire de trois ou de cinq lettres, car ces permutations équivalent à un nombre pair de transpositions.

« Continuons la série des opérations indiquées pour former la valeur x_1 de x.

» On combinera le premier radical avec les coefficients
» de $f(x) = 0$, ou la fonction φ avec des fonctions symé-

» triques des racines, à l'aide des premières opérations
» de l'algèbre, et l'on obtiendra ainsi une fonction des
» racines susceptible de deux valeurs, et, par consé-
» quent, invariable par les permutations circulaires de
» trois lettres. Les radicaux subséquents pourront donner
» encore des fonctions du même genre, s'ils sont du se-
» cond degré. Supposons qu'on soit arrivé à un radical,
» pour lequel la fonction rationnelle équivalente ne soit
» pas invariable par ces permutations. Désignons-le tou-
» jours par

$$y = \varphi(x_1, x_2, x_3, \ldots);$$

» dans l'équation

$$y^n = p$$

» nous ferons encore

$$p = F(x_1, x_2, x_3, \ldots);$$

» cette fonction ne sera plus symétrique, mais seulement
» invariable par les permutations circulaires de trois let-
» tres. Si l'on remplace

$$x_1,\ x_2,\ x_3$$

» par

$$x_2,\ x_3,\ x_1$$

» dans φ, la relation

$$\varphi^n = F$$

» subsistera toujours; et, puisque F ne change pas par
» cette substitution, il viendra

$$\varphi(x_2, x_3, x_1, x_4, \ldots) = \alpha\varphi(x_1, x_2, x_3, x_4, \ldots),$$

» α désignant une racine $n^{\text{ième}}$ de l'unité. » En faisant
dans cette équation la substitution circulaire

$$\begin{pmatrix} x_1, & x_2, & x_3 \\ x_2, & x_3, & x_1 \end{pmatrix},$$

et répétant une seconde fois cette substitution, on aura

$$\varphi(x_3, x_1, x_2, x_4, \ldots) = \alpha\varphi(x_2, x_3, x_1, x_4, \ldots),$$
$$\varphi(x_1, x_2, x_3, x_4, \ldots) = \alpha\varphi(x_3, x_1, x_2, x_4, \ldots),$$

et, en multipliant les trois équations précédentes, « on conclura

$$\alpha^3 = 1.$$

» Ainsi, n sera égal à 3.

» Si le nombre des quantités x_1, x_2, x_3, x_4, etc., est
» supérieur à quatre, ou si l'équation $f(x) = 0$ est d'un
» degré plus élevé que le quatrième, on pourra effectuer
» dans φ une permutation circulaire de cinq lettres, en
» remplaçant

$$x_1, \; x_2, \; x_3, \; x_4, \; x_5$$

» par

$$x_2, \; x_3, \; x_4, \; x_5, \; x_1;$$

» la fonction F ne changera pas, et l'on aura

$$\varphi(x_2, x_3, x_4, x_5, x_1, \ldots) = \alpha\varphi(x_1, x_2, x_3, x_4, x_5, \ldots),$$

» puis, en répétant de part et d'autre la même substi-
» tution,

$$\varphi(x_3, x_4, x_5, x_1, x_2, \ldots) = \alpha\varphi(x_2, x_3, x_4, x_5, x_1, \ldots),$$

....

....

....

» Par la multiplication, on obtient

$$\alpha^5 = 1,$$

» ce qui entraîne

$$\alpha = 1,$$

» puisque α est une racine cubique de l'unité. Ainsi la
» fonction φ est invariable par les permutations circu-
» laires de cinq lettres. » Donc, d'après un théorème démontré dans la dix-neuvième leçon, la fonction φ est aussi invariable par les permutations circulaires de trois lettres.

« Ainsi, *tous les radicaux renfermés dans la racine*

» *d'une équation générale de degré supérieur au qua-*
» *trième devraient être égaux à des fonctions ration-*
» *nelles des racines invariables par les permutations*
» *circulaires de trois racines.* En substituant ces fonc-
» tions dans l'expression de x_1, on arrive à une égalité
» de la forme

$$x_1 = \psi(x_1, x_2, x_3, x_4, x_5, \ldots),$$

» qui doit être identique; ce qui est impossible, puisque
» le second membre reste invariable quand on remplace
» x_1, x_2, x_3, par x_2, x_3, x_1, tandis que le premier change
» évidemment.

» Donc, il est impossible de résoudre par radicaux
» une équation générale du cinquième degré ou de degré
» supérieur.

» La démonstration précédente fait voir en même temps
» que, pour les équations du troisième et du quatrième
» degré, le premier radical, dans l'ordre des opérations,
» doit être un radical carré, et le second un radical
» cubique. Ces circonstances se présentent, en effet, dans
» les formules données par Lagrange et les autres géo-
» mètres. »

VINGT-TROISIÈME LEÇON.

Des nombres congrus ou équivalents. — Théorème de Fermat. — Théorème de Wilson. — Des congruences en général. — Limite des nombres des racines d'une congruence suivant un module premier. — Détermination du nombre de racines d'une congruence. — Nouvelle démonstration du théorème de Wilson.

Des nombres congrus ou équivalents.

Si la différence de deux nombres entiers a et b, positifs ou négatifs, est divisible par un troisième nombre positif p, a et b sont dits *congrus* ou *équivalents*, par rapport à p; le diviseur p est appelé le *module; a* et b sont résidus l'un de l'autre suivant le module p.

Pour exprimer que a et b sont congrus suivant le module p, il suffit d'écrire

$$a = b + \text{un multiple de } p,$$

mais nous adopterons la notation plus commode de M. Gauss, et nous écrirons

$$a \equiv b \quad (\text{mod. } p).$$

Si r désigne le reste de la division de a par p, on a

$$a \equiv r \quad (\text{mod. } p),$$

et le reste r est, si l'on veut, compris entre o et p, ou entre $-\frac{p}{2}$ et $+\frac{p}{2}$; d'où il suit que tout nombre a un résidu inférieur en valeur absolue à la moitié du module. On le nomme *résidu minimum;* mais, si l'on ne veut considérer

que les résidus positifs, les limites seront 0 et p, et le résidu minimum pourra surpasser $\frac{p}{2}$.

L'avantage de la notation de M. Gauss, pour représenter les congruences, consiste surtout en ce qu'elle rappelle la grande analogie qui existe entre les congruences et les égalités, sans qu'il y ait pourtant de confusion à craindre. Nous allons faire voir que la plupart des transformations que l'on peut faire subir aux égalités peuvent être appliquées aux congruences.

Addition et soustraction. — Si l'on a

$$a \equiv b \pmod{p},$$
$$a' \equiv b' \pmod{p},$$

on aura aussi

$$a \pm a' \equiv b \pm b' \pmod{p}.$$

Les congruences proposées expriment, en effet, que

$$a = b + \text{un multiple de } p,$$
$$a' = b' + \text{un multiple de } p;$$

donc

$$a \pm a' = b \pm b' + \text{un multiple de } p,$$

ou

$$a \pm a' \equiv b \pm b' \pmod{p}.$$

Ce qu'il fallait démontrer.

Multiplication. — On peut multiplier une congruence par un nombre quelconque. Car soit

$$a \equiv b \pmod{p},$$

c'est-à-dire

$$a = b + \text{un multiple de } p,$$

on aura aussi

$$ma = mb + \text{un multiple de } p,$$

ou

$$ma \equiv mb \pmod{p}.$$

On peut aussi multiplier entre elles plusieurs con-

gruences de même module. Soient, en effet, deux congruences

$$a \equiv b \pmod{p},$$
$$a' \equiv b' \pmod{p},$$

ou

$$a = b + \text{un multiple de } p,$$
$$a' = b' + \text{un multiple de } p.$$

On aura, en multipliant,

$$aa' = bb' + \text{un multiple de } p,$$

ou

$$aa' \equiv bb' \pmod{p}.$$

Ce qu'il fallait démontrer.

On voit généralement que, si l'on a

$$\left\{\begin{array}{l} a \equiv b, \\ a' \equiv b' \\ \ldots\ldots\ldots \\ a^{(m)} \equiv b^{(m)}, \end{array}\right. \pmod{p},$$

on aura aussi

$$aa' \ldots a^{(m)} \equiv bb' \ldots b^{(m)}.$$

Élévation aux puissances. — On peut élever à une même puissance les deux membres d'une congruence. Cela résulte immédiatement de ce que nous venons de dire au sujet de la multiplication. Si donc on a

$$a \equiv b \pmod{p},$$

on aura aussi

$$a^m \equiv b^m \pmod{p}.$$

Corollaire. — Soit

$$f(x) = Ax^m + Bx^n + \ldots$$

une fonction entière et rationnelle de x, dont les coefficients soient des nombres entiers; si l'on a

$$a \equiv b \pmod{p},$$

on aura aussi

$$f(a) \equiv f(b) \pmod{p}.$$

Division. — On peut diviser une congruence par un nombre quelconque premier avec le module.

Soit, en effet, la congruence

$$ma \equiv mb \pmod{p},$$

ou

$$ma = mb + p \times q,$$

on aura, en divisant par m,

$$a = b + \frac{p \times q}{m},$$

et, si l'on suppose m premier avec p, q devra être divisible par m, et l'on aura

$$a = b + \text{un multiple de } p,$$

ou

$$a \equiv b \pmod{p}.$$

Ce qu'il fallait démontrer.

On peut aussi diviser une congruence par une autre, pourvu que les membres de la seconde soient premiers avec le module. Soient, en effet, les deux congruences

$$(1) \qquad aa' \equiv bb' \pmod{p},$$

$$(2) \qquad a \equiv b \pmod{p}.$$

Désignons par r le résidu minimum de la différence $a' - b'$, on aura

$$(3) \qquad a' \equiv b' \pm r \pmod{p},$$

et, en multipliant (2) et (3),

$$(4) \qquad aa' \equiv bb' \pm br \pmod{p}.$$

Des congruences (1) et (4), on déduit

$$br \equiv 0 \pmod{p},$$

or p est premier avec b par hypothèse, on aura donc

$$r \equiv 0 \pmod{p},$$

ou

$$r = 0,$$

puisque $r < p$. On a donc

$$a' \equiv b' \pmod{p}.$$

Ce qu'il fallait démontrer.

Théorème de Fermat.

Si p est un nombre premier qui ne divise pas a, $a^{p-1} - 1$ est divisible par p ; en d'autres termes, on a

$$a^{p-1} \equiv 1 \pmod{p}.$$

Soient a et p deux nombres premiers entre eux, et considérons les $p - 1$ multiples de a

$$(1) \qquad a,\, 2a,\, 3a, \ldots, (p-1)a;$$

l'un de ces nombres ma, par exemple, ne saurait être divisible par p, puisque p est premier avec a, et qu'il surpasse m. Il en est de même de la différence $ma - m'a$ de deux termes de la suite précédente; car cette différence est elle-même un terme de la suite. Si donc on prend les résidus minima positifs des nombres (1) par rapport à p, ces résidus sont tous différents, et aucun d'eux n'est nul; ce seront donc, dans un certain ordre, les nombres

$$(2) \qquad 1,\, 2,\, 3, \ldots, (p-1).$$

Les nombres (1) étant respectivement congrus aux nombres (2), on aura, en multipliant toutes ces congruences,

$$1.2.3\ldots(p-1)\,a^{p-1} \equiv 1.2.3\ldots(p-1) \pmod{p}.$$

Supposons maintenant que p soit un nombre premier, on pourra diviser la dernière congruence par $1.2.3\ldots p-1$, car ce nombre est premier avec le module, et l'on aura

$$a^{p-1} \equiv 1 \pmod{p}.$$

Ce qu'il fallait démontrer.

Théorème de Wilson.

Si p est un nombre premier, la somme $1.2.3\ldots(p-1)+1$ est divisible par p; en d'autres termes, on a

$$1.2.3\ldots(p-1) \equiv -1 \pmod{p}.$$

Soit a l'un quelconque des nombres

$$(1) \qquad 1, 2, 3, \ldots, (p-1),$$

et formons les multiples de a

$$(2) \qquad a, 2a, 3a, \ldots, (p-1)a.$$

Dans la suite (2), il y a un terme congru à 1, et il n'y en a qu'un seul; supposons que ce soit αa, on aura

$$\alpha a \equiv 1 \pmod{p}.$$

Les nombres a et α sont inégaux, à moins que a ne soit égal à 1 ou à $p-1$. Si, en effet, on a $\alpha = a$, $a^2 - 1 = (a-1)(a+1)$ est divisible par p; or p est premier, il divise donc $a-1$ ou $a+1$, et, comme a est $< p$, on a nécessairement $a = 1$ ou $a = p-1$.

Il résulte de là que les nombres

$$2, 3, 4, \ldots, (p-2),$$

peuvent être associés deux à deux, de manière que le produit de deux *associés* soit congru à l'unité, et, en multipliant entre elles les congruences ainsi obtenues, on aura

$$2.3.4\ldots(p-2) \equiv 1 \pmod{p};$$

multipliant enfin par $p-1$, on a

$$1.2.3.4\ldots(p-1) \equiv p-1 \pmod{p},$$

ou

$$1.2.3.4\ldots(p-1)+1 \equiv 0 \pmod{p}.$$

Ce qu'il fallait démontrer (*).

Remarque. — Ce théorème est surtout remarquable en ce qu'il exprime une propriété qui appartient exclusivement aux nombres premiers; car, si p est un nombre composé, et que θ soit un de ses diviseurs, θ divisera le produit $1.2.3\ldots(p-1)$, et, par conséquent, ne pourra diviser ce même produit augmenté de l'unité. Il en sera donc de même du nombre p.

Des congruences en général.

La théorie des nombres résout sur les congruences le même problème que l'algèbre ordinaire sur les équations; elle se propose, en particulier, de trouver les valeurs de x, qui satisfont à une congruence telle que

$$f(x) \equiv 0 \pmod{p},$$

où $f(x)$ désigne un polynôme entier et rationnel dont les coefficients sont des nombres entiers. Si l'on satisfait à cette congruence, en faisant $x=a$, on y satisfera aussi, d'après une remarque précédente, en faisant, quel que soit l'entier m, $x=a+mp$; d'où il suit que chaque solution en donne une infinité d'autres, mais qui sont toutes équivalentes suivant le module p. Les diverses solutions renfermées dans une même formule $a+mp$ peuvent se

(*) Le théorème de Wilson, ainsi que celui de Fermat, est susceptible d'être généralisé; mais comme cette extension ne nous est d'aucune utilité pour l'objet auquel se rapportent les développements que nous présentons ici, nous nous bornerons à renvoyer le lecteur à l'excellent Mémoire de M. Poinsot. (*Journal de Mathématiques pures et appliquées*, tome X.)

déduire de l'une quelconque d'entre elles; d'ailleurs, on peut disposer de l'entier m de manière que $a + mp$ soit compris entre $-\frac{p}{2}$ et $+\frac{p}{2}$, ou entre o et p; il n'y a donc lieu de s'occuper que des solutions comprises entre ces limites.

Cela posé, nous appellerons *racines* de la congruence

$$f(x) \equiv 0 \pmod{p},$$

les diverses valeurs de x comprises entre o et p, qui rendent $f(x)$ divisible par p.

Une congruence est *identique* si tous ses coefficients sont divisibles par le module, et elle est évidemment impossible si ses coefficients sont divisibles par le module, à l'exception du terme indépendant de x.

Si $F(x)$ désigne un polynôme entier et rationnel, ayant pour coefficients des nombres entiers, on peut substituer à la congruence

$$f(x) \equiv 0 \pmod{p}$$

la congruence équivalente

$$f(x) + pF(x) \equiv 0 \pmod{p},$$

et disposer ensuite des coefficients indéterminés de $F(x)$, pour rabaisser au-dessous de p, et même de $\frac{p}{2}$ si l'on veut, tous les coefficients de la congruence.

Nous nous bornerons, dans ce qui va suivre, aux congruences dont le module est premier. On peut alors faire en sorte que le coefficient du premier terme soit égal à l'unité.

Considérons, en effet, la congruence

$$A_0 x^m + A_1 x^{m-1} + A_2 x^{m-2} + \ldots \equiv 0 \pmod{p},$$

dont le module p est supposé premier, et les coefficients

A_0, A_1, A_2, etc., compris entre o et p, ou entre $-\frac{p}{2}$ et $+\frac{p}{2}$. En ajoutant à son premier membre le polynôme

$$p(y_1 x^{m-1} + y_2 x^{m-2} + \ldots),$$

on peut l'écrire ainsi :

$$A_0 x^m + (A_1 + py_1) x^{m-1} + (A_2 + py_2) x^{m-2} + \ldots \equiv 0 \pmod{p},$$

ou

$$A_0 \left(x^m + \frac{A_1 + py_1}{A_0} x^{m-1} + \frac{A_2 + py_2}{A_0} x^{m-2} + \ldots \right) \equiv 0 \pmod{p}.$$

Cela posé, A_0, étant inférieur à p, sera premier avec lui, et on pourra disposer des indéterminées y_1, y_2, etc., de manière que

$$\frac{A_1 + py_1}{A_0}, \quad \frac{A_2 + py_2}{A_0}, \ldots$$

soient des nombres entiers B_1, B_2, etc., compris entre o et p ou entre $-\frac{p}{2}$ et $+\frac{p}{2}$; notre congruence sera donc

$$A_0(x^m + B_1 x^{m-1} + B_2 x^{m-2} + \ldots) \equiv 0 \pmod{p},$$

ou, comme A_0 est premier avec le module,

$$x^m + B_1 x^{m-1} + B_2 x^{m-2} + \ldots \equiv 0 \pmod{p}.$$

Limite du nombre des racines d'une congruence suivant un module premier.

Théorème. — *Une congruence non identique, suivant un module premier, a au plus autant de racines qu'il y a d'unités dans son degré.*

Soit la congruence de degré m

(1) $$f(x) \equiv 0 \pmod{p},$$

où le coefficient du premier terme est l'unité. Supposons que a soit une racine, divisons $f(x)$ par $x-a$, et désignons par $f_1(x)$ le quotient qui est du degré $m-1$, on aura

$$f(x) = (x-a)\,f_1(x) + f(a);$$

et comme $f(a)$ est, par hypothèse, divisible par p, la congruence (1) peut s'écrire ainsi :

$$(x-a)\,f_1(x) \equiv 0 \pmod{p}.$$

Soit maintenant b une seconde racine, on aura

$$(b-a)f_1(b) \equiv 0 \pmod{p},$$

ou

$$f_1(b) \equiv 0 \pmod{p};$$

car $b-a$ est inférieur à p, et, par conséquent, premier avec lui; b est donc racine de

(2) $$f_1(x) \equiv 0 \pmod{p},$$

dont le premier terme a, comme celui de (1), pour coefficient l'unité.

Il résulte de là que la congruence (1) de degré m ne peut avoir qu'une racine de plus que la congruence (2) du degré $m-1$. A son tour, cette dernière ne pourra avoir qu'une racine de plus qu'une congruence

(3) $$f_2(x) \equiv 0 \pmod{p}$$

de degré $m-2$, et dont le premier terme a pour coefficient l'unité. Par suite, la proposée (1) ne peut avoir que deux racines de plus que (3), et en continuant ce raisonnement, on fera voir que la congruence (1) ne peut avoir que $m-1$ racines de plus qu'une congruence du premier degré, telle que

$$x - l \equiv 0 \pmod{p},$$

laquelle n'admet que la seule racine l. D'où il suit, enfin.

qu'une congruence de degré m ne peut avoir plus de m racines; mais elle peut en avoir moins de m, et même n'en avoir aucune.

Corollaire I. — Supposons que la congruence de degré m

$$f(x) \equiv 0 \pmod{p},$$

dont le premier terme a pour coefficient l'unité, ait effectivement m racines

$$a,\ b,\ c,\ldots,\ k,\ l:$$

ces m racines appartiendront aussi à la congruence

$$f(x) - (x-a)(x-b)\ldots(x-l) \equiv 0 \pmod{p};$$

mais cette dernière n'est que du degré $m-1$, elle est donc identique et, par conséquent, on a

$$f(x) = (x-a)(x-b)\ldots(x-l) + p\,F(x),$$

$F(x)$ désignant une fonction entière et rationnelle de x dont les coefficients sont des nombres entiers.

Corollaire II. — D'après le théorème de Fermat, la congruence

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

admet les $p-1$ racines

$$1,\ 2,\ 3,\ldots,\ (p-1).$$

Il suit de là que si $f(x)$ désigne un diviseur du binôme $x^{p-1}-1$, ou, plus généralement, de ce même binôme augmenté d'un polynôme $pF(x)$ de degré $p-1$, la congruence

$$f(x) \equiv 0 \pmod{p}$$

aura autant de racines qu'il y a d'unités dans son degré.

Soit, en effet,

$$x^{p-1} - 1 + p\,F(x) \equiv f(x) f_1(x);$$

la congruence de degré $p-1$

$$f(x)\,f_1(x) \equiv 0 \pmod{p}$$

admet les racines

$$1,\ 2,\ 3,\ldots,\ (p-1).$$

D'ailleurs ces racines sont celles des deux suivantes :

$$f(x) \equiv 0 \pmod{p}, \quad f_1(x) \equiv 0 \pmod{p},$$

et si l'une d'elles avait moins de racines qu'il n'y a d'unités dans son degré, il faudrait que l'autre en eût plus qu'il n'y a d'unités dans le sien, ce qui est impossible.

Détermination du nombre des racines d'une congruence.

Ce dernier corollaire fournit un moyen très-aisé de déterminer le nombre de racines d'une congruence de module premier. Démontrons d'abord le lemme suivant.

Lemme. — *Si $f_2(x)$ désigne le reste de la division des deux polynômes $f(x)$ et $f_1(x)$ dont les premiers termes ont pour coefficients l'unité, les racines communes aux deux congruences*

$$f(x) \equiv 0 \pmod{p}, \quad f_1(x) \equiv 0 \pmod{p}$$

sont les mêmes que les racines communes à

$$f_1(x) \equiv 0 \pmod{p}, \quad f_2(x) \equiv 0 \pmod{p}.$$

Soit Q le quotient de la division de $f(x)$ par $f_1(x)$, on aura

$$f(x) = f_1(x).\mathrm{Q} + f_2(x),$$

et cette égalité fait voir que si $f_1(x)$ est divisible par p en même temps que l'un des deux polynômes $f(x)$ et $f_2(x)$, l'autre le sera nécessairement aussi ; d'où résulte la proposition énoncée.

Corollaire. — Les racines communes à deux congruences

$$f(x) \equiv 0 \pmod{p}, \quad f_1(x) \equiv 0 \pmod{p}$$

appartienent à la congruence

$$\varphi(x) \equiv 0 \pmod{p},$$

$\varphi(x)$ désignant le plus grand commun diviseur aux deux polynômes $f(x)$ et $f_1(x)$.

Remarque. — Pour trouver ce plus grand commun diviseur $\varphi(x)$, on suivra la marche ordinaire; seulement on fera en sorte, comme il a été indiqué page 305, que les premiers termes des restes aient tous pour coefficients l'unité.

Problème. — *Trouver le nombre des racines d'une congruence*

$$(1) \qquad f(x) \equiv 0 \pmod{p}.$$

Les racines de cette congruence appartiennent toutes à la congruence.

$$(2) \qquad x^{p-1} - 1 \equiv 0 \pmod{p}.$$

Il suffit donc de chercher les racines communes aux congruences (1) et (2). Pour cela, on prendra, comme il vient d'être dit, le plus grand commun diviseur à $f(x)$ et à $x^{p-1} - 1$. S'il n'existe pas de diviseur commun, la proposée n'aura aucune racine; si, au contraire, on trouve un plus grand commun diviseur $\varphi(x)$ de degré μ, la congruence proposée aura μ racines, qui seront celles de

$$\varphi(x) \equiv 0 \pmod{p}.$$

Cette dernière a effectivement μ racines, puisque $\varphi(x)$ est un diviseur de degré μ du binôme $x^{p-1} - 1$.

Nouvelle démonstration du théorème de Wilson.

Si p est premier, la congruence

$$(x-1)(x-2)(x-3)\ldots(x-p+1)-(x^{p-1}-1)\equiv 0 \pmod{p}$$

admet les $p-1$ racines

$$1,\ 2,\ 3,\ldots,\ (p-1);$$

et comme elle n'est que du degré $p-2$, en ordonnant son premier membre par rapport à x, les coefficients devront être tous divisibles par p. Si donc on désigne par S_1 la somme des nombres $1, 2,\ldots, (p-1)$, par S_2 la somme de leurs produits deux à deux, etc., par S_{p-1} leur produit, on aura

$$S_1\equiv 0,\quad S_2\equiv 0,\quad S_3\equiv 0,\ldots,\ S_{p-1}\equiv -1,$$

suivant le module p. La dernière de ces congruences constitue le théorème de Wilson.

VINGT-QUATRIÈME LEÇON.

Propriétés des racines des congruences binômes de module premier. — De l'existence des racines primitives. — Du nombre des racines primitives. — Recherche des racines primitives d'un nombre premier. — Table des racines primitives des nombres premiers inférieurs à 100. — Propriété des racines de l'équation $x^m - 1 = 0$, dont le degré m est un nombre premier.

Propriétés des racines des congruences binômes de module premier.

I. *Les racines communes à deux congruences binômes de module premier p,*

$$x^m \equiv 1 \pmod{p}, \quad x^n \equiv 1 \pmod{p},$$

sont également racines de la congruence

$$x^\theta \equiv 1 \pmod{p},$$

θ étant le plus grand commun diviseur de m et n.

$x^\theta - 1$ est, en effet, le plus grand commun diviseur de $x^m - 1$ et de $x^n - 1$. Ce théorème est, par suite, une conséquence du corollaire démontré page 309.

Il est évident que, réciproquement, chaque racine de la congruence $x^\theta - 1 \equiv 1$ satisfait aux deux proposées.

Corollaire. — Les racines d'une congruence binôme de module premier

$$x^m \equiv 1 \pmod{p},$$

appartenant, d'après le théorème de Fermat, à la con-

gruence

$$x^{p-1} \equiv 1 \pmod{p},$$

sont aussi racines de la congruence

$$x^{\theta} \equiv 1 \pmod{p},$$

θ désignant le plus grand commun diviseur des nombres m et $p-1$.

Comme $x^{\theta}-1$ est un diviseur de $x^{p-1}-1$, cette dernière a précisément θ racines, ainsi que la proposée.

Si m est premier avec $p-1$, on a $\theta=1$, et alors la congruence $x^m \equiv 1$ n'a d'autre racine que l'unité.

D'après ce qui précède, on peut borner l'étude des congruences binômes de la forme

$$x^m \equiv 1 \pmod{p},$$

à celles dont le degré m est un diviseur de $p-1$.

II. *Si a désigne une racine quelconque de la congruence de module premier*

$$x^m \equiv 1 \pmod{p}$$

dont le degré m est un diviseur de $p-1$, toute puissance de a ou son résidu minimum est également racine.

La congruence

$$a^m \equiv 1 \pmod{p}$$

entraîne, en effet,

$$a^{mk} \equiv 1, \quad \text{ou} \quad (a^k)^m \equiv 1,$$

et si b désigne le résidu minimum de a^k, par rapport à p, on a

$$a^k \equiv b, \quad \text{d'où} \quad b^m \equiv 1;$$

et, par conséquent, tous les termes de la série

$$a, \; a^2, \; a^3, \ldots,$$

ou leurs résidus minima, sont racines de la même con-

gruence. Or, à cause de $a^m \equiv 1$, on a aussi

$$a^{m+1} \equiv a, \quad a^{m+2} \equiv a^2, \ldots.$$

La série précédente contient donc au plus m termes ayant des résidus différents, et ces résidus se reproduisent périodiquement de m en m. Si les m premiers termes

$$a, \; a^2, \; a^3, \ldots, \; a^{m-1}, \; a^m \text{ ou } 1$$

sont différents (incongrus suivant le module p), leurs résidus sont les m racines de la congruence proposée.

Dans le cas contraire, si l'on a, par exemple,

$$a^{n+n'} \equiv a^{n'} \pmod{p},$$

a étant premier avec p, il vient, en divisant par $a^{n'}$,

$$a^n \equiv 1 \pmod{p},$$

et, par conséquent, a est racine d'une congruence binôme

$$x^n \equiv 1 \pmod{p}$$

de degré n inférieur à m.

Il résulte de là que *si a est une racine de la congruence $x^m \equiv 1 \pmod{p}$, qui n'appartienne à aucune congruence de degré moindre $x^n \equiv 1 \pmod{p}$, les m racines de la proposée sont les résidus des m puissances de a*

$$a, \; a^2, \; a^3, \ldots, \; a^{m-1}, \; a^m.$$

Cela posé, nous appellerons *racines primitives* d'une congruence binôme

$$x^m \equiv 1 \pmod{p}$$

dont le degré m divise $p-1$, celles des racines de cette congruence qui n'appartiennent à aucune congruence de même forme et de degré moindre. Chaque racine primitive jouit de la propriété de donner toutes les autres racines par ses diverses puissances.

Remarque. — Toute racine non primitive, appartenant

à une congruence de même forme et de degré moindre, appartient aussi à une troisième congruence de même forme, et dont le degré divise celui de la proposée.

De l'existence des racines primitives

Considérons la congruence

$$(1) \qquad x^m \equiv 1 \pmod{p},$$

et supposons d'abord que m ne contienne qu'un seul facteur premier q, que l'on ait

$$m = q^\mu;$$

toute racine non primitive de

$$(2) \qquad x^{q^\mu} \equiv 1$$

appartient à une congruence

$$x^\theta \equiv 1$$

dont le degré θ est un diviseur de q^μ et même de $q^{\mu-1}$; et, par conséquent, appartient aussi à

$$(3) \qquad x^{q^{\mu-1}} \equiv 1.$$

D'ailleurs les racines de (3) sont toutes racines de (2); leur nombre est $q^{\mu-1}$, par conséquent, celui des racines primitives de la proposée est

$$q^\mu - q^{\mu-1}, \quad \text{ou} \quad q^\mu\left(1 - \frac{1}{q}\right).$$

Supposons maintenant m quelconque, et soit

$$m = q^\mu r^\nu \ldots s^\lambda,$$

$q, r, \ldots, s$ désignant des facteurs premiers inégaux.

Considérons les congruences

(4) $x^{q^\mu} \equiv 1 \pmod{p},\quad x^{r^\nu} \equiv 1 \pmod{p},\ldots,\quad x^{s^\lambda} \equiv 1 \pmod{p},$

et désignons par a une racine primitive de la première, par b une de la seconde, etc., par c une de la dernière; je dis que le résidu du produit

$$ab\ldots c$$

est une racine primitive de la proposée

(5) $$x^{q^\mu r^\nu \ldots s^\lambda} \equiv 1 \pmod{p}.$$

Il est d'abord évident que $ab\ldots c$, ou son résidu, est racine, car ayant

$$a^{q^\mu} \equiv 1,\quad b^{r^\nu} \equiv 1,\ldots,\quad c^{s^\lambda} \equiv 1 \pmod{p},$$

on a aussi

$$(ab\ldots c)^{q^\mu r^\nu \ldots s^\lambda} \equiv 1 \pmod{p}.$$

Maintenant, si ce produit n'est pas une racine primitive de la proposée, il sera racine d'une congruence

$$x^\theta \equiv 1 \pmod{p},$$

dont le degré θ sera un diviseur de m, et il y aura au moins l'un des facteurs premiers de m, qui entrera dans θ moins de fois que dans m. Admettons que le facteur q soit dans ce cas, alors θ divisera $q^{\mu-1} r^\nu \ldots s^\lambda$, et, par suite, $ab\ldots c$ sera racine de la congruence

$$x^{q^{\mu-1} r^\nu \ldots s^\lambda} \equiv 1 \pmod{p};$$

on aura donc

$$(ab\ldots c)^{q^{\mu-1} r^\nu \ldots s^\lambda} \equiv 1;$$

mais on a aussi

$$(b\ldots c)^{q^{\mu-1}r^{\nu}\ldots s^{\lambda}} \equiv 1,$$

et, par la division,

$$a^{q^{\mu-1}r^{\nu}\ldots s^{\lambda}} \equiv 1.$$

On voit, par là, que a est racine des deux congruences

$$x^{q^{\mu-1}r^{\nu}\ldots s^{\lambda}} \equiv 1 \quad \text{et} \quad x^{q^{\mu}} \equiv 1,$$

et, par suite, de

$$x^{q^{\mu-1}} \equiv 1,$$

puisque $q^{\mu-1}$ est le plus grand commun diviseur entre les degrés des précédentes; a n'est donc pas, comme on l'a supposé, une racine primitive de $x^{q^{\mu}} \equiv 1 \pmod{p}$.

Il est ainsi démontré que, si $a, b, \ldots, c$ désignent des racines primitives, respectivement de la première, de la deuxième, etc., de la dernière des congruences (4), le produit $ab\ldots c$, ou son résidu, est une racine primitive de la congruence proposée (5).

Ce qui précède démontre l'existence d'une racine primitive pour toute congruence binôme de module premier

$$x^m \equiv 1 \pmod{p},$$

mais on n'en peut pas immédiatement conclure le nombre de ces racines. Toutefois, par des raisonnements semblables à ceux que nous avons employés dans la treizième leçon à l'occasion de l'équation binôme, on prouverait aisément que toutes les racines, tant primitives que non primitives de la congruence (5), sont représentées par la formule

$$ab\ldots c,$$

où l'on doit prendre pour $a, b, \ldots, c$ toutes les racines respectivement de la première des congruences (4), de la deuxième, etc., de la dernière; et que la même formule donne toutes les racines primitives, en prenant pour $a, b, \ldots, c$ les diverses racines primitives des congruences auxquelles elles appartiennent. Comme le nombre des racines primitives a est $q^\mu\left(1-\frac{1}{q}\right)$, celui des racines b, $r^\nu\left(1-\frac{1}{r}\right), \ldots,$ celui des racines c, $s^\lambda\left(1-\frac{1}{s}\right)$, on en conclurait que le nombre des racines primitives de la proposée est

$$m\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\cdots\left(1-\frac{1}{s}\right).$$

On sait que ce même nombre (*voir* la *Théorie des nombres*, ou le Mémoire déjà cité de M. Poinsot) exprime combien il y a de nombres premiers et inférieurs à m.

Je ne crois pas nécessaire de développer ces raisonnements, que le lecteur trouvera aisément après avoir étudié la treizième leçon; mais j'indiquerai la démonstration ingénieuse de M. Poinsot pour prouver qu'en admettant l'existence d'une racine primitive de la congruence

$$x^m \equiv 1 \pmod{p},$$

il y en a précisément autant que de nombres inférieurs et premiers à m.

Du nombre des racines primitives.

Soit a une racine primitive de la congruence

$$x^m \equiv 1 \pmod{p},$$

et formons la suite des m puissances

$$(1) \qquad a,\ a^2,\ a^3, \ldots,\ a^{m-1},\ a^m,$$

dont les résidus sont les m racines de la proposée. Si l'on considère un nombre quelconque e inférieur et premier à m, et qu'après avoir rangé ces racines en cercle, on les considère en allant de l'une à l'autre de e en e, comme l'intervalle e par lequel on saute, est premier à m, on sera obligé de passer par toutes les racines avant de revenir à la racine a, d'où l'on est parti : donc la suite

$$a^e\ (a^e)^2\ (a^e)^3 \ldots\ (a^e)^{m-1}\ (a^e)^m$$

donne, aux multiples près de p, toutes les racines de la proposée, donc a^e est une racine primitive.

Si le nombre e, que nous avons supposé premier avec p, avait avec lui un plus grand commun diviseur $\theta > 1$, en opérant, sur la suite (1), comme nous venons de le faire, on ne passerait jamais que par un nombre $\frac{m}{\theta}$ de racines, et, par conséquent, a^e ne serait pas une racine primitive.

Il suit évidemment de là que la congruence proposée a autant de racines primitives qu'il y a de nombres premiers et inférieurs à m.

Recherche des racines primitives d'un nombre premier.

On nomme *racines primitives d'un nombre premier p* les racines primitives de la congruence binôme de degré $p-1$

$$x^{p-1} \equiv 1 \pmod{p}.$$

Théorème. — *Soient x_1 et ξ deux nombres compris entre* 0 *et p, et θ un diviseur de $p-1$; si l'on a*

$$x_1^\theta \equiv \xi \pmod{p},$$

on a aussi

$$\xi^{\frac{p-1}{\theta}} \equiv 1 \pmod{p};$$

et, réciproquement, si l'on a

$$\xi^{\frac{p-1}{\theta}} \equiv 1 \pmod{p},$$

la congruence

$$x^\theta \equiv \xi \pmod{p}$$

a θ racines.

La première partie du théorème est évidente; car, si l'on a

$$x_1^\theta \equiv \xi \pmod{p},$$

en élevant les deux membres à la puissance $\frac{p-1}{\theta}$, on a

$$x_1^{p-1} \equiv \xi^{\frac{p-1}{\theta}} \pmod{p},$$

et, à cause du théorème de Fermat,

$$\xi^{\frac{p-1}{\theta}} \equiv 1.$$

Réciproquement, supposons que l'on ait $\xi^{\frac{p-1}{\theta}} \equiv 1$, ou

$$\xi^{\frac{p-1}{\theta}} - 1 = pQ;$$

retranchant chaque membre de cette égalité de $x^{p-1} - 1$, il vient

$$x^{p-1} - 1 - pQ = x^{p-1} - \xi^{\frac{p-1}{\theta}} = (x^\theta)^{\frac{p-1}{\theta}} - \xi^{\frac{p-1}{\theta}}.$$

Or le second membre admet pour diviseur $x^\theta - \xi$; il en est donc de même du premier membre $x^{p-1} - 1 - pQ$, et, par conséquent, en vertu d'un théorème démontré dans la dernière leçon (page 307), la congruence

$$x^\theta - \xi \equiv 0 \pmod{p}$$

a θ racines. Ce qu'il fallait démontrer.

Corollaire. — Si p est un nombre premier, et qu'en décomposant $p-1$ en facteurs premiers, on ait

$$p-1=2^{\rho}q^{\mu}r^{\nu}\dots s^{\lambda},$$

les racines non primitives de la congruence

$$x^{p-1}-1\equiv 0 \pmod{p},$$

lesquelles appartiennent nécessairement à l'une des congruences

$$x^{\frac{p-1}{2}}\equiv 1,\quad x^{\frac{p-1}{q}}\equiv 1,\quad x^{\frac{p-1}{r}}\equiv 1,\dots,\quad x^{\frac{p-1}{s}}\equiv 1,$$

sont, en vertu du théorème précédent, des résidus de carrés (*), ou de puissances q, ou de puissances r, etc., ou de puissances s; et, réciproquement, tout nombre résidu d'un carré, ou d'une puissance q, ou etc., est racine de l'une des congruences précédentes, et n'est pas racine primitive du nombre premier p.

On voit aussi que, parmi les nombres

$$1,\ 2,\ 3,\dots,p-1,$$

il y en a la moitié qui sont des carrés (résidus de carrés), la $q^{ième}$ partie qui sont des puissances q, la $r^{ième}$ partie des puissances r, etc., la $s^{ième}$ partie des puissances s; et, plus généralement, si l'on ne considère parmi ces nombres que ceux qui sont à la fois des puissances $2, q, r,\dots,$ la $s^{ième}$ partie de ces derniers seront en même temps des puissances s. En effet, les nombres qui sont à la fois des résidus de carrés de puissances q, de puissances r, etc.,

(*) Les résidus de carrés ou de cubes suivant le module p sont appelés *résidus quadratiques et cubiques*; ils jouent un rôle important dans la théorie des nombres.

satisfont aux congruences

$$x^{\frac{p-1}{2}} \equiv 1,\quad x^{\frac{p-1}{q}} \equiv 1,\quad x^{\frac{p-1}{r}} \equiv 1, \ldots, \pmod{p},$$

et, par conséquent, sont racines de

$$x^{\frac{p-1}{2qr\ldots}} \equiv 1 \pmod{p}:$$

leur nombre est donc $\frac{p-1}{2qr\ldots}$; pareillement, le nombre de ceux qui sont en même temps des puissances s est $\frac{p-1}{2qr\ldots s}$, il est donc la $s^{\text{ième}}$ partie du premier.

Problème. — *Trouver les racines primitives d'un nombre premier.*

Le théorème que nous venons de démontrer fournit un moyen très-simple de trouver les racines primitives d'un nombre premier.

Soient p un nombre premier; $2, q, r, \ldots, s$ les facteurs premiers inégaux de $p-1$, et écrivons les $p-1$ nombres

$$1,\ 2,\ 3,\ 4, \ldots, p-1;$$

si l'on enlève de cette suite tous les résidus de carrés, de puissances q, de puissances r, etc., il ne restera plus que les racines primitives de p.

Au moyen des carrés, on exclut d'abord la moitié des nombres, ainsi que nous l'avons établi plus haut; au moyen des puissances q, on exclura la $q^{\text{ième}}$ partie de ceux qui restent, et ainsi de suite. Cette méthode, pour trouver les racines primitives d'un nombre premier, fournit une démonstration nouvelle du théorème relatif au nombre de ces racines; ce nombre sera en effet, d'après ce qui précède,

$$(p-1)\left(1-\frac{1}{2}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\cdots\left(1-\frac{1}{s}\right).$$

Nous allons montrer, par deux exemples, comment il faut faire l'application du procédé qu'on vient d'indiquer.

PREMIER EXEMPLE. — *Trouver les racines primitives de* 17.

Nous écrivons d'abord les seize nombres

$$(1)\quad 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16,$$

et comme 16 n'admet que le facteur premier 2, il suffit d'ôter de cette suite les nombres qui sont résidus quadratiques. Pour cela, nous élèverons ces nombres au carré; mais, comme on a généralement

$$(17 - h)^2 \equiv h^2 \pmod{17},$$

les huit derniers carrés donneront les mêmes résidus que les huit premiers: il suffit donc d'élever au carré les huit premiers, on trouvera ainsi

$$1,\ 4,\ 9,\ 16,\ 25,\ 36,\ 49,\ 64,$$

qui ont pour résidus

$$1,\ 4,\ 9,\ 16,\ 8,\ 2,\ 15,\ 13,$$

et en effaçant ces huit résidus de la suite (1), il restera les huit racines primitives de 17, savoir

$$3,\ 5,\ 6,\ 7,\ 10\ 11,\ 12,\ 14.$$

SECOND EXEMPLE. — *Trouver les racines primitives de* 31.

Écrivons les trente nombres

$$(1)\quad \left\{\begin{matrix} 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, & 10, \\ 11, & 12, & 13, & 14, & 15, & 16, & 17, & 18, & 19, & 20, \\ 21, & 22, & 23, & 24, & 25, & 26, & 27, & 28, & 29, & 30; \end{matrix}\right.$$

comme les facteurs premiers de 30 sont 2, 3 et 5, il suf-

fira d'enlever de la suite (1) les résidus quadratiques cubiques et de cinquièmes puissances.

Pour exclure les carrés, nous élèverons les quinze premiers nombres (1) au carré, ce qui donne

1, 4, 9, 16, 25, 36, 49, 64, 81, 100,
121, 144, 169, 196, 225:

ces carrés ont pour résidus

(2) 1, 4, 9, 16, 25, 5, 18, 2, 19, 7, 28, 20, 14, 10, 8;

ôtant ces quinze nombres (2) de la suite (1), il restera les quinze que voici :

(3) 3, 6, 11, 12, 13, 15, 17, 21, 22, 23, 24, 26, 27, 29, 30,

dont il faut maintenant supprimer les cubes et les cinquièmes puissances. Chaque nombre déjà supprimé (2) satisfait à la congruence

$$x^{15} \equiv 1 \pmod{31};$$

donc sa puissance troisième et sa puissance cinquième y satisfont aussi, et, par conséquent, font partie des nombres déjà supprimés. D'après cela, les nombres de la suite (3) qu'il reste à rejeter sont des résidus de puissances troisième et cinquième de ces mêmes nombres (3). Pour avoir les résidus des cubes de la suite (3), il suffit de multiplier les premières puissances par les résidus carrés que la suite (2) fait connaître, et qui sont

9, 5, 28, 20, 14, 8, 10, 7, 19, 2, 18, 25, 16, 4, 1;

on aura ainsi les résidus cubiques suivants :

27, 30, 308, 240, 182, 120, 170, 147, 418,
46, 432, 650, 432, 116, 30,

dont les résidus minima sont

$$(4)\qquad \begin{cases} 27,\ 30,\ 29,\ 23,\ 27,\ 27,\ 15,\ 23, \\ 15,\ 15,\ 29,\ 30,\ 29,\ 23,\ 30. \end{cases}$$

Il n'y en a que cinq de différents, comme nous le savions d'avance, ce sont

$$(5)\qquad 15,\ 23,\ 27,\ 29,\ 30,$$

et en ôtant ces nombres de la suite (3), il ne restera plus que les dix suivants :

$$(6)\qquad 3,\ 6,\ 11,\ 12,\ 13,\ 17,\ 21,\ 22,\ 24,\ 26,$$

dont il n'y a plus à rejeter que ceux qui sont des cinquièmes puissances. Chacun des nombres déjà exclus satisfait à l'une des congruences

$$x^{15} \equiv 1 \pmod{31}, \quad x^{10} \equiv 1 \pmod{31};$$

il en est donc de même de la cinquième puissance, qui, par conséquent, fait partie des nombres exclus : un nombre de la suite (6) ne peut donc être la cinquième puissance que d'un nombre de la même suite. Pour avoir les résidus des cinquièmes puissances des nombres (6), il suffit de multiplier les résidus cubiques déjà formés par les résidus quadratiques correspondants, et de prendre les résidus minima des produits. Les résidus cubiques sont

$$27,\ 30,\ 29,\ 23,\ 27,\ 15,\ 23,\ 15,\ 29,\ 30,$$

les quadratiques

$$9,\ 5,\ 28,\ 20,\ 14,\ 10,\ 7,\ 19,\ 18,\ 25;$$

les produits sont

$$243,\ 150,\ 812,\ 460,\ 378,\ 150,\ 161,\ 285,\ 522,\ 750,$$

et l'on trouve pour résidus des cinquièmes puissances

$$26,\ 26,\ 6,\ 26,\ 6,\ 26,\ 6,\ 6,\ 26,\ 6.$$

Il n'y a ainsi, dans la suite (6), que deux cinquièmes puissances, comme nous le savions déjà, savoir

$$6,\ 26;$$

en supprimant ces deux nombres, il ne restera plus que les huit racines primitives de 31, savoir

$$3,\ 11,\ 12,\ 13,\ 17,\ 21,\ 22,\ 24.$$

La Table suivante renferme les racines primitives des nombres premiers inférieurs à 100.

Propriétés des racines de l'équation $\frac{x^m-1}{x-1}=0$, *où m est premier.*

Soit α une racine imaginaire de l'équation

(1) $$x^m = 1$$

de degré m premier; les $m-1$ racines de l'équation

(2) $$\frac{x^m-1}{x-1}=0$$

sont, comme on sait,

$$\alpha,\ \alpha^2,\ \alpha^3,\ldots,\ \alpha^{m-1}.$$

Soit maintenant a une racine primitive du nombre premier m, ou de la congruence

$$x^{m-1}\equiv 1 \pmod{m};$$

les $m-1$ racines de cette congruence, savoir

$$1,\ 2,\ 3,\ldots,\ (m-1),$$

peuvent être représentées par les diverses puissances de a,

$$1,\ a,\ a^2,\ldots,\ a^{m-2},$$

aux multiples près de m; et, par conséquent, les $m-1$ racines de l'équation (2) sont

$$\alpha,\ \alpha^a,\ \alpha^{a^2},\ldots,\ \alpha^{a^{m-2}},$$

en sorte que chacune d'elles s'obtient en élevant la précédente à la puissance a, et la même chose a lieu encore à cause de $a^{m-1}\equiv 1 \pmod{m}$, si l'on range en cercle ces m racines, et que l'on considère successivement chacune d'elles comme étant la première. D'après cela,

si x désigne l'une quelconque des racines de l'équation (2), et que l'on fasse

$$x' = \theta(x),\ \ \theta\theta(x) = \theta^2(x),\ \ \theta\theta^2(x) = \theta^3(x), \ldots,$$

les m racines de l'équation (2) seront représentées par

$$x,\ \ \theta(x),\ \ \theta^2(x), \ldots,\ \ \theta^{m-2}(x),$$

et l'on aura

$$\theta^{m-1}(x) = x.$$

C'est sur cette propriété que repose la méthode de M. Gauss pour la résolution de l'équation (2), dont nous nous occuperons dans une prochaine leçon.

VINGT-CINQUIÈME LEÇON.

Théorèmes sur les nombres.

Les principes exposés dans les deux leçons précédentes suffisent pour établir un grand nombre de théorèmes curieux et utiles. Je me propose ici de démontrer quelques-uns de ces théorèmes, et je renverrai, pour plus de détails, à la *Théorie des Nombres* de Legendre, et aux *Recherches arithmétiques* de M. Gauss.

Théorème I.

Le produit de deux nombres de la forme $a^2 + nb^2$ est aussi de la même forme.

On a, en effet, identiquement

$$(a^2 + nb^2)(c^2 + nd^2) = (ac \pm nbd)^2 + n(ad \mp bc)^2.$$

Corollaire. — Le produit de tant de nombres qu'on voudra de la forme $a^2 + nb^2$, est aussi de la même forme; et, en particulier, le produit de plusieurs nombres formés chacun par l'addition de deux carrés est lui-même la somme de deux carrés.

Théorème II.

Le produit de deux sommes de quatre carrés est aussi une somme de quatre carrés.

Soient α, β, α', β', γ, δ, γ', δ' des nombres quelconques;

on a identiquement

$$(1)\left\{\begin{array}{l}(\alpha\beta'-\beta\alpha')(\gamma\delta'-\delta\gamma')\\=(\alpha\gamma+\alpha'\gamma')(\beta\delta+\beta'\delta')-(\alpha\delta+\alpha'\delta')(\beta\gamma+\beta'\gamma')\text{ [*]}.\end{array}\right.$$

Cela posé, faisons

$$\begin{array}{ll}\alpha=a+b\sqrt{-1}, & \gamma=p+q\sqrt{-1},\\ \beta=c+d\sqrt{-1}, & \delta=r+s\sqrt{-1},\\ \alpha'=-(c-d\sqrt{-1}), & \gamma'=-(r-s\sqrt{-1}),\\ \beta'=a-b\sqrt{-1}, & \delta'=p-q\sqrt{-1};\end{array}$$

l'équation (1) devient

$$(2)\left\{\begin{array}{l}(a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2)\\=(pa-qb+rc-sd)^2+(qa+pb-sc-rd)^2\\+(ra-sb-pc+qd)^2+(sa+rb+qc+pd)^2.\end{array}\right.$$

Ce qu'il fallait démontrer.

Ce beau théorème d'algèbre est dû à Euler. La démonstration précédente m'a été communiquée par M. Hermite. Il est bon de remarquer que l'équation (2) peut être écrite de plusieurs manières différentes, car on a le droit de changer les signes des quantités a, b, c, d, p, q, r, s à volonté.

Corollaire. — Le produit de tant de sommes de quatre carrés que l'on voudra est aussi une somme de quatre carrés.

Théorème III.

Tout nombre qui divise la somme de deux carrés premiers entre eux est lui-même la somme de deux carrés.

On a de cette proposition un grand nombre de démons-

(*) Cette équation est comprise, comme cas particulier, dans un théorème plus général sur les *déterminants*.

trations. J'en ai publié récemment une nouvelle à laquelle j'ai été conduit par quelques recherches sur la théorie des nombres (*); mais la plus simple que je connaisse est due à M. Hermite : c'est celle que je vais présenter ici.

Si un nombre divise une somme de deux carrés premiers entre eux, on peut toujours supposer que l'un de ces carrés soit l'unité. Supposons, en effet, que p divise

$$a^2 + b^2,$$

il divisera aussi, quels que soient les entiers x et y, le produit

$$(a^2 + b^2)(x^2 + y^2) \quad \text{ou} \quad (ax + by)^2 + (ay - bx)^2.$$

Or a et b étants premiers entre eux, on peut choisir x et y, de manière que l'on ait

$$ay - bx = 1,$$

et alors p divisera

$$(ax + by)^2 + 1,$$

c'est-à-dire une somme de deux carrés dont l'un est égal à l'unité.

Il est bon de remarquer qu'à la place de $ax + by$, on peut prendre son résidu minimum q, par rapport à p, et $q^2 + 1$ sera divisible par p, q étant compris entre 0 et $\frac{p}{2}$.

Je dis maintenant que si p divise $q^2 + 1$, p est la somme de deux carrés. Réduisons, en effet, $\frac{q}{p}$ en fraction continue, et poussons l'opération jusqu'à ce qu'on obtienne deux réduites consécutives

$$\frac{m}{n}, \quad \frac{m'}{n'}$$

(*) *Journal de Mathématiques pures et appliquées*, tome XIII.

telles, que l'on ait $n < \sqrt{p}$, mais $n' > \sqrt{p}$. Cela est toujours possible, car la première de toutes les réduites a 1 pour dénominateur, et la dernière p lui-même.

La différence entre $\frac{q}{p}$ et $\frac{m}{n}$ est moindre, comme on sait, que $\frac{1}{nn'}$; on a donc

$$\left(\frac{q}{p} - \frac{m}{n}\right)^2 < \frac{1}{n^2 n'^2}, \quad \text{ou} \quad (nq - mp)^2 < \frac{p^2}{n'^2};$$

mais, pas hypothèse, n'^2 est $> p$: donc

$$(nq - mp)^2 < p.$$

Ajoutant cette inégalité, membre à membre, avec

$$n^2 < p,$$

il vient

$$(nq - mp)^2 + n^2 < 2p.$$

Or le premier membre de cette inégalité,

$$n^2(q^2 + 1) - 2mnqp + m^2p^2,$$

est divisible par p, puisque $q^2 + 1$ l'est par hypothèse, il est donc nécessairement égal à p, et l'on a

$$p = (nq - mp)^2 + n^2;$$

d'où il suit que p est effectivement la somme de deux carrés.

THÉORÈME IV.

Tout nombre qui divise la somme d'un carré et du double d'un carré est lui-même la somme d'un carré et du double d'un carré.

Ce théorème se démontre de la même manière que le précédent.

Je dis d'abord que, si p divise a^2+2b^2, on peut supposer $b=1$. En effet, p, divisant a^2+2b^2, divisera aussi

$$(a^2+2b^2)(x^2+2y^2) \quad \text{ou} \quad (ax+2by)^2+2(ay-bx)^2,$$

quels que soient x et y. Or a et b étant supposés premiers entre eux, on peut faire

$$ay-bx=1,$$

et, en appelant q le résidu minimum de $ax+2by$ par rapport à p, on voit que q^2+2 est divisible par p.

Cela posé, réduisons $\frac{q}{p}$ en fraction continue, et soient, comme dans le précédent théorème,

$$\frac{m}{n}, \quad \frac{m'}{n'}$$

deux réduites consécutives telles, que $n<\sqrt{p}$, et $n'>\sqrt{p}$, on a, comme plus haut, les deux inégalités

$$(nq-mp)^2<p,$$
$$n^2<p;$$

ajoutant la première de ces inégalités avec le double de la seconde, il vient

$$(nq-mp)^2+2n^2<3p.$$

Mais le premier membre est divisible par p, puisque q^2+2 l'est, il est donc égal à p ou à $2p$. Dans le premier cas, p est la somme d'un carré et du double d'un carré. Supposons que l'on ait

$$2p=(nq-mp)^2+2n^2,$$

cette égalité exige que $nq-mp$ soit pair, et, en divisant par 2, on a

$$p=n^2+2\left(\frac{nq-mp}{2}\right)^2.$$

Donc, dans tous les cas, p a la forme $a^2 + 2b^2$. Ce qu'il fallait démontrer.

THÉORÈME V.

Tout nombre qui divise la différence entre un carré et le double d'un carré est lui-même la différence entre un carré et le double d'un carré.

Supposons que p divise

$$\pm(a^2 - 2b^2),$$

il divisera aussi, quels que soient x et y,

$$(a^2 - 2b^2)(x^2 - 2y^2) \quad \text{ou} \quad (ax + 2by)^2 - 2(ay - bx)^2.$$

On peut déterminer les entiers x et y de manière qu'on ait

$$ay - bx = 1,$$

et, en désignant par q le résidu de $ax + by$, on voit que p divise

$$q^2 - 2.$$

Cela posé, réduisons $\frac{q}{p}$ en fraction continue, et désignons par

$$\frac{m}{n}, \quad \frac{m'}{n'}$$

deux réduites consécutives telles, que $n < \sqrt{p}$, mais $n' > \sqrt{p}$, on aura, comme précédemment,

$$(nq - mp)^2 < p,$$
$$2n^2 < 2p;$$

d'où il suit que la différence

$$2n^2 - (nq - mp)^2$$

est inférieure à $2p$, et, comme elle est divisible par p, et

que d'ailleurs elle est positive, on a

$$p = 2n^2 - (nq - mp)^2.$$

Ce qu'il fallait démontrer.

Nous avons admis comme évident que $2n^2 - (nq - mp)^2$ est positif; car, si le contraire avait lieu, on aurait

$$(nq - mp)^2 - 2n^2 < p,$$

ce qui est impossible, puisque le premier membre est, par hypothèse, divisible par p, et qu'il ne peut évidemment pas être nul.

Théorème VI.

Tout nombre qui divise la somme de quatre carrés premiers entre eux est lui-même la somme de quatre carrés.

Supposons que p divise

$$A^2 + B^2 + C^2 + D^2,$$

et soient a, b, c, d les résidus minima, compris entre o et $\frac{p}{2}$, de A, B, C, D, qu'on peut prendre avec le signe + ou —; p divisera

$$a^2 + b^2 + c^2 + d^2.$$

Posons

$$(1) \qquad a^2 + b^2 + c^2 + d^2 = pp';$$

a, b, c, d étant moindres que $\frac{p}{2}$, on aura $pp' < 4\left(\frac{p}{2}\right)^2$; ou

$$p' < p.$$

Si l'on avait $p' = 1$, p serait la somme de quatre carrés, et le théorème serait démontré; supposons donc $p' > 1$. Comme p' divise $a^2 + b^2 + c^2 + d^2$, il divisera aussi

$$(a - \alpha p')^2 + (b - 6p')^2 + (c - \gamma p')^2 + (d - \delta p')^2,$$

et si l'on détermine α, β, γ, δ de manière que chacun de ces carrés soit moindre que $\frac{p'^2}{4}$, on pourra écrire

$$(2) \quad (a-\alpha p')^2+(b-\beta p')^2+(c-\gamma p')^2+(d-\delta p')^2=p'p'',$$

avec

$$p''<p'.$$

Multipliant ensemble les équations (1) et (2), et se servant de l'équation (2) du théorème II, il vient

$$\begin{aligned}&(a\delta-b\gamma+c\beta-d\alpha)^2p'^2+(a\gamma+b\delta-c\alpha-d\beta)^2p'^2\\&+(a\beta-b\alpha-c\delta+d\gamma)^2p'^2\\&+[a^2+b^2+c^2+d^2-(a\alpha+b\beta+c\gamma+d\delta)p']^2=pp'^2p'';\end{aligned}$$

divisant par p'^2, et ayant égard à l'équation (1), on a

$$\begin{aligned}&(a\delta-b\gamma+c\beta-d\alpha)^2+(a\gamma+b\delta-c\alpha-d\beta)^2\\&+(a\beta-b\alpha-c\delta+d\gamma)^2+(p-a\alpha-b\beta-c\gamma-d\delta)^2=pp'',\end{aligned}$$

ou, pour abréger,

$$(3) \quad a'^2+b'^2+c'^2+d'^2=pp''.$$

Cette équation (3) a la même forme que (1), seulement p'' est $<p'$. Si l'on a $p''=1$, l'équation (3) montre que p est la somme de quatre carrés, et le théorème est démontré. Sinon, en opérant sur l'équation (3) comme nous avons fait sur l'équation (1), on obtiendra une nouvelle équation de la forme

$$a''^2+b''^2+c''^2+d''^2=pp''',$$

où

$$p''' \text{ sera } < p'';$$

et l'on peut continuer de cette manière jusqu'à ce qu'on obtienne une équation de la forme

$$a^{(n)2}+b^{(n)2}+c^{(n)2}+d^{(n)2}=p,$$

ce qui arrivera nécessairement, puisque les nombres

$$p',\ p'',\ p''',\ldots$$

sont des entiers qui vont en décroissant; d'où il suit enfin que le nombre p est la somme de quatre carrés.

THÉORÈME VII.

Tout nombre premier $4n+1$ *est la somme de deux carrés.*

Première démonstration. — Soit p un nombre premier $4n+1$, la congruence

$$x^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$$

a $\frac{p-1}{2}$ racines; désignons par q l'une d'elles, on a

$$q^{2n} + 1 \equiv 0 \pmod{p},$$

d'où il suit que p divise la somme de deux carrés, et est, par suite, la somme de deux carrés.

Seconde démonstration. — On peut aussi déduire ce théorème de celui de Wilson. En effet, par le théorème de Wilson, p divise la somme

$$(1.2.3\ldots 2n)[(2n+1)\ldots 4n]+1;$$

mais les nombres

$$2n+1,\quad 2n+2,\ldots,\quad 4n$$

sont respectivement congrus à

$$-2n,\quad -(2n-1),\ldots,\quad -1$$

suivant le module p; donc le produit des premiers est congru au produit des seconds. D'ailleurs le nombre des facteurs étant pair, on peut changer leurs signes, et l'on a

$$(1.2.3\ldots 2n)^2 + 1 \equiv 0 \pmod{p};$$

p divise ainsi la somme de deux carrés, et, par conséquent, est lui-même la somme de deux carrés.

Remarque. — Un nombre de la forme $4n + 3$ ne peut être la somme de deux carrés. En effet, tout carré pair a la forme $4n$, et tout carré impair la forme $4n + 1$; par conséquent, la somme de deux carrés a toujours l'une des deux formes $4n$ et $4n + 1$.

Corollaire. — Si un nombre composé ne contient que le facteur premier 2 et des facteurs premiers de la forme $4n + 1$, il est nécessairement la somme de deux carrés; et réciproquement, si un nombre composé est la somme de deux carrés, il ne contient que des facteurs premiers égaux à 2 ou de la forme $4n + 1$.

Théorème VIII.

Un nombre premier $4n + 1$ n'est la somme de deux carrés que d'une seule manière.

Nous allons faire voir que si un nombre impair p est décomposable de deux manières différentes en deux carrés, p ne peut être un nombre premier. Supposons, en effet, que l'on ait

$$p = a^2 + b^2 = c^2 + d^2,$$

a et b étant différents de c et d; p étant impair, des deux nombres a et b, ou c et d, l'un est pair et l'autre impair. Nous supposerons a et c pairs, b et d impairs. Cela posé, on a

$$a^2 - c^2 = d^2 - b^2,$$

ou

$$\frac{a+c}{d+b} = \frac{d-b}{a-c}.$$

Désignons par $\frac{A}{B}$ la valeur de la fraction irréductible équivalente à chacune des précédentes, on aura

$$a + c = 2\rho A, \quad d + b = 2\rho B,$$
$$d - b = 2\lambda A, \quad a - c = 2\lambda B.$$

ρ et λ étant des nombres entiers ; par suite, on aura

$$a = \rho A + \lambda B, \quad c = \rho A - \lambda B,$$
$$b = \rho B - \lambda A, \quad d = \rho B + \lambda A,$$

et, par conséquent,

$$p = (\rho A + \lambda B)^2 + (\rho B - \lambda A)^2,$$

ou

$$p = (\rho^2 + \lambda^2)(A^2 + B^2).$$

p n'est donc pas un nombre premier, puisqu'il admet les deux diviseurs $\rho^2 + \lambda^2$ et $A^2 + B^2$; donc un nombre premier ne peut être la somme de deux carrés que d'une seule manière.

Remarque. — Un nombre composé peut être la somme de deux carrés de plusieurs manières.

Soit, par exemple, le nombre p produit de deux nombres premiers $4n + 1$, l'un égal à $a^2 + b^2$, l'autre à $c^2 + d^2$, on aura

$$p = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$
$$= (ad + bc)^2 + (ac - bd)^2,$$

et notre nombre p se trouve ainsi décomposé en deux carrés de deux manières qui seront, en général, différentes. Ainsi

$$65 = 64 + 1 = 49 + 16.$$

Théorème IX.

Tout nombre premier de l'une des formes $8n + 1$ et $8n + 3$, est la somme d'un carré et du double d'un carré.

1°. Soit p un nombre premier $8n + 1$. La congruence

$$x^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$$

a $\frac{p-1}{2}$ ou $4n$ racines, puisque son premier membre divise $x^{p-1}-1$, et en désignant par q l'une de ces racines, on a

$$q^{4n}+1 \equiv 0 \pmod{p},$$

ou

$$(q^{2n}-1)^2+2q^{2n} \equiv 0 \pmod{p}.$$

On voit donc que p divise la somme d'un carré et du double d'un carré, donc (théorème IV) p est lui-même de la forme a^2+2b^2.

2°. Soit p un nombre premier $8n+3$, p divisera

$$(2^{4n+1}-1)(2^{4n+1}+1),$$

d'après le théorème de Fermat. Or le premier facteur $2.2^{4n}-1$ est la différence entre un carré et le double d'un autre; donc s'il était divisible par p, p aurait la forme (théorème V)

$$\pm(a^2-2b^2);$$

mais cette forme ne peut appartenir à aucun nombre $8n+3$, les carrés ayant la forme $4n$ ou $4n+1$: d'où il suit que p ne peut diviser $2^{4n+1}-1$; il divisera donc l'autre facteur

$$2.2^{4n}+1$$

qui est la somme d'un carré et du double d'un carré, et, par conséquent, p aura aussi la forme

$$a^2+2b^2.$$

Remarque I. — En combinant ce théorème avec le théorème VII, on voit que tout nombre premier de la forme $8n+1$ a en même temps les deux formes a^2+b^2 et a^2+2b^2.

Remarque II. — Aucun nombre $8n+5$ ou $8n+7$ ne peut être de la forme a^2+2b^2.

THÉORÈME X.

Quel que soit le nombre premier p, on peut toujours trouver deux entiers t et u compris entre o et $\frac{p}{2}$, et tels, que

$$t^2 + u^2 + 1,$$

soit divisible par p.

Ce théorème se trouve démontré par ce qui précède, si $p = 4n + 1$; car, dans ce cas, il divise un nombre $q^2 + 1$, qu'on déduit de la forme précédente, en faisant $t = 0$, $u = q$.

Il en est de même si $p = 8n + 3$; mais nous allons démontrer généralement le théorème pour tout nombre premier $p = 4n + 3$.

On a vu, dans la vingt-quatrième leçon, que, parmi les racines

$$1,\ 2,\ 3, \ldots,\ p-1,$$

de la congruence

$$(1) \qquad x^{p-1} \equiv 1 \pmod{p},$$

il y en a $\frac{p-1}{2}$ qui appartiennent à

$$(2) \qquad x^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

et $\frac{p-1}{2}$ à

$$(3) \qquad x^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Les racines de la congruence (2) sont résidus quadratiques par rapport à p; au contraire, celles de la congruence (3) sont non résidus quadratiques.

Cela posé, comme le premier terme de la suite

$$1,\ 2,\ 3, \ldots,\ p-1$$

est résidu quadratique, et qu'il y a autant de résidus que de non résidus quadratiques, il y a nécessairement dans cette suite un résidu a suivi d'un non résidu $a+1$. Posons d'abord

$$(4) \qquad a \equiv t^2 \pmod{p};$$

ensuite $a+1$, étant non résidu quadratique, satisfait à la congruence (3), et, comme $\frac{p-1}{2}$ est impair, puisque $p = 4n+3$, on a

$$(-a-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p};$$

d'où il suit que $-a-1$ est résidu quadratique: on peut donc poser

$$(5) \qquad -a-1 \equiv u^2 \pmod{p}.$$

Ajoutant les congruences (4) et (5), il vient

$$t^2 + u^2 + 1 \equiv 0 \pmod{p}.$$

Ce qu'il fallait démontrer.

Théorème XI.

Tout nombre premier est la somme de quatre ou d'un moindre nombre de carrés.

Car tout nombre premier divise une somme de trois carrés t^2+u^2+1, laquelle est comprise dans la forme plus générale $a^2+b^2+c^2+d^2$. On peut donc dire que tout nombre premier divise une somme de quatre carrés, et, par suite, en vertu du théorème VI, tout nombre premier est la somme de quatre carrés, ou d'un moindre nombre; car quelques-uns de ces carrés peuvent être nuls.

THÉORÈME XII.

Tout nombre entier est la somme de quatre ou d'un moindre nombre de carrés.

En effet, tous les facteurs premiers impairs d'un nombre entier sont de la forme

$$a^2 + b^2 + c^2 + d^2;$$

il en est de même du facteur premier 2. Par conséquent, en vertu du théorème II, le produit de tous ces facteurs premiers, c'est-à-dire le nombre proposé, a aussi la forme

$$a^2 + b^2 + c^2 + d^2.$$

VINGT-SIXIÈME LEÇON.

Des équations irréductibles dont deux racines sont tellement liées entre elles, que l'une puisse s'exprimer rationnellement par l'autre. Sur la résolution de ces équations.

Nous avons démontré, dans la vingt-deuxième leçon, l'impossibilité de résoudre algébriquement les équations générales de degré supérieur au quatrième. Mais une équation de degré quelconque, dont les coefficients ont des valeurs particulières déterminées, peut, dans certains cas, être résolue algébriquement (*). Ainsi, les équations auxquelles conduit le problème de la division du cercle en un nombre premier de parties égales sont toujours résolubles par radicaux, comme M. Gauss l'a établi dans ses recherches arithmétiques. Ces équations ont cette propriété, que chaque racine peut s'exprimer rationnellement par l'une quelconque des autres (*voyez* treizième leçon). Abel, en partant de cette remarque, a fait voir que, si deux racines d'une équation irréductible sont tellement liées entre elles, que l'une puisse s'exprimer rationnellement

(*) Gallois a donné la condition nécessaire et suffisante pour qu'une équation irréductible de degré premier soit résoluble par radicaux. *Journal de Mathématiques pures et appliquées*, tome X). Mon ami M. Liouville m'a annoncé l'intention où il était de publier un jour des développements relatifs à ce remarquable travail. Ce n'est que par ces développements, dont M. Liouville a bien voulu me communiquer une partie, que je suis parvenu à comprendre certains points du Mémoire de Gallois, dont la lecture ne peut être abordée que par les géomètres qui se sont occupés d'une manière toute spéciale de la théorie des équations. On voit par quelle réserve je suis empêché de présenter ici la découverte de Gallois

par l'autre, on peut toujours ramener la résolution de l'équation à celle d'équations de degrés moindres. Il y a même des cas où l'équation est résoluble algébriquement; cela arrive en particulier si son degré est un nombre premier.

Nous allons exposer ici ces recherches d'Abel, et nous ferons ensuite l'application de sa méthode aux équations de la division du cercle en un nombre premier de parties égales.

Des équations irréductibles dont deux racines sont tellement liées entre elles, que l'une puisse s'exprimer rationnellement par l'autre.

Lemme. — *Si* $f(x) = 0$ *est une équation irréductible,* $F(x)$ *une fonction rationnelle, et que l'équation* $F(x) = 0$ *admette une racine* x_1 *de* $f(x) = 0$*, elle admettra aussi toutes les autres.*

Soit, en effet,

$$F(x) = \frac{\varphi(x)}{\psi(x)},$$

φ et ψ désignant des fonctions entières; la racine x_1 sera, par hypothèse, commune aux équations

$$f(x) = 0, \quad \varphi(x) = 0;$$

et cela exige que le polynôme $\varphi(x)$ soit divisible par $f(x)$, car autrement il y aurait un diviseur commun à ces polynômes, et l'équation $f(x) = 0$ ne serait pas irréductible. Soit donc

$$\varphi(x) = f(x)\,\varpi(x),$$

on aura

$$F(x) = \frac{\varpi(x)}{\psi(x)} f(x),$$

et, par conséquent, l'équation $F(x) = 0$ admettra toutes les racines de $f(x) = 0$.

Soit maintenant

$$(1) \qquad f(x) = 0$$

une équation irréductible de degré μ, et supposons que deux racines x' et x_1 soient liées entre elles par l'équation

$$x' = \theta x_1,$$

où θx désigne une fonction rationnelle de x et de quantités connues. x' étant racine de l'équation (1), on aura

$$f(\theta x_1) = 0;$$

d'où il suit que x_1 sera racine de l'équation

$$(2) \qquad f(\theta x) = 0,$$

et, par conséquent, cette équation (2) admettra toutes les racines de l'équation (1), car celle-ci est irréductible, et $f(\theta x)$ est une fonction rationnelle. En d'autres termes, si x désigne une racine quelconque de l'équation (1), θx sera aussi racine de cette équation. Mais θx_1 est racine de l'équation (1); donc $\theta\theta x_1$ le sera aussi, ainsi que $\theta\theta\theta x_1$, et généralement, en répétant sur x_1 un nombre quelconque de fois l'opération désignée par θ, on obtiendra toujours une racine de l'équation (1).

Soit, pour abréger,

$$\theta\theta x_1 = \theta^2 x_1, \quad \theta\theta^2 x_1 = \theta^3 x_1, \quad \theta\theta^3 x_1 = \theta^4 x_1, \ldots,$$

tous les termes de la série

$$(3) \qquad x_1, \theta x_1, \theta^2 x_1, \theta^3 x_1, \ldots$$

seront des racines de l'équation (1). Mais la série (3) renferme une infinité de termes, tandis que l'équation (1) n'a que μ racines; il faut donc que quelques-unes des quantités (3) se trouvent répétées un nombre infini de fois.

Supposons, par exemple, que l'on ait

$$\theta^{m+n} x_1 = \theta^m x_1,$$

ou

$$\theta^n (\theta^m x_1) - \theta^m x_1 = 0,$$

l'équation

$$\theta^n x - x = 0$$

a la racine $\theta^m x_1$ commune avec l'équation (1); elle admettra donc toutes les racines de l'équation (1), et l'on aura

$$\theta^n x_1 - x_1 = 0,$$

ou

$$\theta^n x_1 = x_1.$$

On tire de là

$$\theta^{n+k} x_1 = \theta^k x_1;$$

d'où il suit qu'à partir du $n^{ième}$ les termes de la série (3) se reproduiront dans le même ordre, et que cette série ne contiendra que ces n quantités distinctes

$$(4) \qquad x_1,\ \theta x_1,\ \theta^2 x_1, \ldots,\ \theta^{n-1} x_1.$$

Ces n quantités seront, en effet, distinctes, si n est le nombre de fois qu'il faut répéter sur x_1 l'opération désignée par θ pour reproduire x_1.

Si l'on a $\mu = n$, la série (4) contient toutes les racines de l'équation (1); ce cas est celui de l'équation

$$\frac{x^{n+1} - 1}{x - 1} = 0,$$

où $n + 1$ est un nombre premier, ainsi que nous l'avons établi dans la vingt-quatrième leçon.

Supposons $\mu > n$, et soit x_2 une racine de l'équation (1) qui ne fasse pas partie de la série (4), on fera voir, comme précédemment, que toutes les quantités

$$(5) \qquad x_2,\ \theta x_2,\ \theta^2 x_2, \ldots,\ \theta^{n-1} x_2, \ldots$$

sont également racines de l'équation (1). Or je dis que,

dans la série (5), les n premiers termes

$$(6)\qquad x_2,\ \theta x_2,\ \theta^2 x_2,\ \ldots,\ \theta^{n-1} x_2$$

sont les seuls qui peuvent être différents. En effet, l'équation

$$\theta^n x - x = 0$$

admet la racine x_1 de l'équation (1); donc elle admettra toutes les autres, et l'on aura

$$\theta^n x_2 = x_2,$$

d'où

$$\theta^{n+k} x_2 = \theta^k x_2.$$

Par conséquent, les termes de la série (5) se reproduiront dans le même ordre, à partir du $n^{\text{ième}}$, et les seuls de ces termes qui peuvent être distincts sont renfermés dans la série (6).

Je dis maintenant que les termes de la série (6) sont effectivement différents entre eux, et distincts des quantités (4).

L'égalité

$$\theta^k x_2 = \theta^i x_2,$$

où k et i sont inférieurs à n, est effectivement impossible; car, d'après le lemme établi au commencement de cette leçon, elle entraînerait

$$\theta^k x_1 = \theta^i x_1,$$

ce qui n'a pas lieu, puisque les quantités (4) sont différentes.

L'égalité

$$\theta^k x_2 = \theta^i x_1$$

est de même impossible. Si, en effet, elle avait lieu, il en résulterait

$$\theta^{n-k}\theta^i x_1 = \theta^{n-k}\theta^k x_2,$$

ou

$$\theta^{n-k+i} x_1 = \theta^n x_2 = x_2,$$

et, par conséquent, x_2 ferait partie de la série (4), ce qui est contre l'hypothèse.

Le nombre de racines de l'équation (1) renfermées dans les séries (4) et (6) est $2n$, on a donc nécessairement $\mu = 2n$ ou $\mu > 2n$.

Supposons $\mu > 2n$, et désignons par x_3 une racine de l'équation (1) qui ne fasse pas partie des groupes (4) et (6); en raisonnant comme précédemment, on formera un troisième groupe de n racines

$$x_3,\ \theta x_3,\ \theta^2 x_3,\ \ldots,\ \theta^{n-1} x_3,$$

toutes distinctes et différentes des quantités (3) et (6); d'où il suit nécessairement que l'on a $\mu = 3n$ ou $\mu > 3n$.

En continuant ainsi, on verra que les μ racines de l'équation (1) peuvent être partagées en un certain nombre m de groupes composés chacun de n termes, en sorte que

$$\mu = mn.$$

Les racines de l'équation (1) seront alors

$$(7)\quad \left\{\begin{array}{l} x_1,\ \theta x_1,\ \theta^2 x_1,\ \ldots,\ \theta^{n-1} x_1, \\ x_2,\ \theta x_2,\ \theta^2 x_2,\ \ldots,\ \theta^{n-1} x_2, \\ x_3,\ \theta x_3,\ \theta^2 x_3,\ \ldots,\ \theta^{n-1} x_3, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_m,\ \theta x_m,\ \theta^2 x_m,\ \ldots,\ \theta^{n-1} x_m. \end{array}\right.$$

Considérons l'équation de degré n ayant pour racines les racines de l'un de ces groupes, du premier, par exemple, et soit

$$(x - x_1)(x - \theta x_1)(x - \theta^2 x_1)\ldots(x - \theta^{n-1} x_1) = 0,$$

ou

$$(8)\quad x^n + A'_1 x^{n-1} + A'_2 x^{n-2} + \ldots + A'_{n-1} x + A'_n = 0$$

cette équation. Les coefficients

$$A'_1, \; A'_2, \ldots, \; A'_n$$

sont des fonctions rationnelles et symétriques des quantités

$$x_1, \; \theta x_1, \; \theta^2 x_1, \ldots, \; \theta^{n-1} x_1,$$

et ne dépendent, comme on va voir, que d'une seule équation du degré m.

Soit, en effet, y_1 une fonction rationnelle et symétrique quelconque des quantités

$$(9) \qquad x_1, \; \theta x_1, \; \theta^2 x_1, \ldots, \; \theta^{n-1} x_1;$$

θx_1, $\theta^2 x_1$, etc., étant des fonctions rationnelles de x_1, y_1 le sera aussi, et nous poserons

$$y_1 = F(x_1),$$

F désignant une fonction rationnelle. En outre, à cause de $\theta^n x_1 = x_1$, les quantités (9) ne feront que se changer les unes dans les autres si l'on remplace x_1 par θx_1, $\theta^2 x_1, \ldots, \theta^{n-1} x_1$, et comme y_1 est une fonction symétrique de ces quantités, sa valeur sera invariable par ces changements; on aura donc

$$y_1 = F(x_1) = F(\theta x_1) = F(\theta^2 x_1) = \ldots = F(\theta^{n-1} x_1).$$

Désignons par

$$y_2, \; y_3, \ldots, \; y_m$$

les valeurs que prend y_1 quand on y remplace x_1 successivement par

$$x_2, \; x_3, \ldots, \; x_m,$$

on aura

$$y_2 = F(x_2) = F(\theta x_2) = F(\theta^2 x_2) = \ldots = F(\theta^{n-1} x_2),$$

. . . .

. . . .

$$y_m = F(x_m) = F(\theta x_m) = F(\theta^2 x_m) = \ldots = F(\theta^{n-1} x_m).$$

Soit maintenant

$$(y-y_1)(y-y_2)\ldots(y-y_m)=0,$$

ou

$$(10)\quad y^m+p_1y^{m-1}+p_2y^{m-2}+\ldots+p_{m-1}y+p_m=0$$

l'équation qui a pour racines $y_1, y_2,\ldots, y_m$; je dis que les coefficients p_1, p_2, etc., de cette équation peuvent être exprimés rationnellement par les coefficients de l'équation proposée (1). On a, en effet, quel que soit l'entier λ,

$$y_1^\lambda=\frac{1}{n}\left\{[F(x_1)]^\lambda+[F(\theta x_1)]^\lambda+\ldots+[F(\theta^{n-1}x_1)]^\lambda\right\},$$

$$y_2^\lambda=\frac{1}{n}\left\{[F(x_2)]^\lambda+[F(\theta x_2)]^\lambda+\ldots+[F(\theta^{n-1}x_2)]^\lambda\right\},$$

. . . .

. . . .

$$y_m^\lambda=\frac{1}{n}\left\{[F(x_m)]^\lambda+[F(\theta x_m)]^\lambda+\ldots+[F(\theta^{n-1}x_m)]^\lambda\right\},$$

et, en ajoutant,

$$y_1^\lambda+y_2^\lambda+\ldots+y_m^\lambda=\frac{1}{n}\sum[F(x)]^\lambda;$$

le signe $\sum$ du second membre s'étendant à toutes les racines de l'équation proposée, ce second membre est donc une fonction symétrique et rationnelle de toutes ces racines; d'où il résulte que les sommes de puissances semblables des racines de l'équation (10) peuvent être exprimées rationnellement par les coefficients de l'équation proposée. On pourra donc aussi exprimer de la même manière les coefficients p_1, p_2, etc., comme nous l'avions annoncé.

La fonction rationnelle et symétrique y_1 des quantités (9), qui peut d'ailleurs être choisie à volonté, dépend donc directement d'une équation de degré m. D'ailleurs

les fonctions

$$y_1, A'_1, A'_2, \ldots, A'_n$$

sont des fonctions semblables; car elles peuvent toutes être considérées comme des fonctions rationnelles de la seule racine x_1. On pourra donc exprimer

$$A'_1, A'_2, \ldots, A'_n$$

en fonction rationnelle de y_1.

Nous sommes ainsi conduits à l'une des applications les plus importantes de la théorie des fonctions semblables, que nous avons développée dans une précédente leçon; mais, comme cette théorie est sujette à quelques cas d'exception, il ne sera pas inutile d'entrer, avec Abel, dans le détail du calcul des coefficients A'_1, A'_2, etc.

Désignons par $\psi(x_1)$ l'un quelconque de ces coefficients; ψ est une fonction rationnelle qui ne doit pas changer quand on remplace x_1 par $\theta x_1, \theta^2 x_1, \ldots, \theta^{n-1} x_1$, puisque $\psi(x_1)$ est, comme y_1, une fonction symétrique des quantités (9); et il en sera de même de la fonction

$$y_1^\lambda \psi(x_1) \quad \text{ou} \quad [F(x_1)]^\lambda \psi(x_1).$$

On aura donc

$$y_1^\lambda \psi(x_1) = \frac{1}{n} \left\{ \begin{array}{l} [F(x_1)]^\lambda \psi(x_1) + [F(\theta x_1)]^\lambda \psi(\theta x_1) + \ldots \\ + [F(\theta^{n-1} x_1)]^\lambda \psi(\theta^{n-1} x_1) \end{array} \right\};$$

en remplaçant x_1 successivement par $x_2, x_3, \ldots, x_m$, on aura des expressions semblables pour $y_2^\lambda \psi(x_2), \ldots, y_m^\lambda \psi(x_m)$, et si l'on pose

$$(11) \qquad t_\lambda = y_1^\lambda \psi(x_1) + y_2^\lambda \psi(x_2) + \ldots + y_m^\lambda \psi(x_m),$$

on aura

$$t_\lambda = \frac{1}{n} \sum [F(x)]^\lambda \psi(x),$$

le signe $\sum$ s'étendant à toutes les racines de l'équation (1).

On voit, par là, que t_λ est une fonction symétrique et rationnelle des racines de l'équation (1), qui pourra, par conséquent, s'exprimer rationnellement en fonction des quantités connues.

Cela posé, en donnant à λ les valeurs $0, 1, 2, 3, \ldots, (m-1)$, l'équation (11) donnera les suivantes :

$$(12)\quad\left\{\begin{array}{l} \psi(x_1) + \psi(x_2) + \ldots + \psi(x_m) = t_0, \\ y_1\psi(x_1) + y_2\psi(x_2) + \ldots + y_m\psi(x_m) = t_1, \\ y_1^2\psi(x_1) + y_2^2\psi(x_2) + \ldots + y_m^2\psi(x_m) = t_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ y_1^{m-1}\psi(x_1) + y_2^{m-1}\psi(x_2) + \ldots + y_m^{m-1}\psi(x_m) = t_{m-1}, \end{array}\right.$$

dont les seconds membres peuvent être considérés comme connus.

Pour avoir la valeur de $\psi(x_1)$, ajoutons les équations (12) après les avoir respectivement multipliées par les indéterminées

$$R_0,\quad R_1, \ldots, R_{m-2},\quad 1,$$

et faisons, pour abréger,

$$(13)\quad \varphi(y) = y^{m-1} + R_{m-2}\,y^{m-2} + \ldots + R_1 y + R_0,$$

on aura

$$\begin{aligned} &\varphi(y_1)\psi(x_1) + \varphi(y_2)\psi(x_2) + \ldots \varphi(y_m)\psi(x_m) \\ &= t_0 R_0 + t_1 R_1 + \ldots + t_{m-2} R_{m-2} + t_{m-1}; \end{aligned}$$

et si l'on détermine les facteurs R_0, R_1, etc., par les conditions

$$\varphi(y_2) = 0,\quad \varphi(y_3) = 0, \ldots, \varphi(y_m) = 0,$$

on aura

$$(14)\qquad \psi(x_1) = \frac{t_0 R_0 + t_1 R_1 + \ldots + t_{m-2} R_{m-2} + t_{m-1}}{\varphi(y_1)}.$$

Cherchons maintenant les valeurs de R_0, R_1, etc. D'après notre hypothèse, l'équation

$$\varphi(y) = 0$$

doit avoir pour racines $y_2, y_3, \ldots, y_m$, mais ces racines appartiennent aussi à l'équation (10), qui admet en outre la racine y_1, on aura donc

$$(15)\quad \left\{\begin{aligned}
\varphi(y) &= \frac{y^m + p_1 y^{m-1} + p_2 y^{m-2} + \ldots + p_{m-1} y + p_m}{y - y_1} \\
&= y^{m-1} \begin{array}{l} + p_1 \\ + y_1 \end{array}\Bigg| \; y^{m-2} \begin{array}{l} + p_2 \\ + p_1 y_1 \\ + y_1^2 \end{array}\Bigg| \; y^{m-3} + \ldots \begin{array}{l} + p_{m-1} \\ + p_{m-2} y \\ + \ldots\ldots \\ \ldots\ldots\ldots \\ + p_1 y_1^{m-2} \\ + y_1^{m-1}. \end{array}
\end{aligned}\right.$$

Comparant les valeurs $\varphi(y)$ données par les équations (13) et (15), on trouve

$$(16)\qquad \left\{\begin{aligned}
R_{m-2} &= p_1 + y_1, \\
R_{m-3} &= p_2 + p_1 y_1 + y_1^2, \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
R_1 &= p_{m-2} + p_{m-3} y_1 + \ldots + y_1^{m-2}, \\
R_0 &= p_{m-1} + p_{m-2} y_1 + \ldots + y_1^{m-1}.
\end{aligned}\right.$$

On tire aussi de l'équation (15)

$$\varphi'(y_1) = m y_1^{m-1} + (m-1) p_1 y_1^{m-2} + \ldots + 2 p_{m-2} y_1 + p_{m-1},$$

et en faisant, pour abréger,

$$\begin{aligned}
T_0 &= t_0 p_{m-1} + t_1 p_{m-2} + \ldots + t_{m-2} p_1 + t_{m-1},\\
T_1 &= t_0 p_{m-2} + t_1 p_{m-3} + \ldots + t_{m-2},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
T_{m-2} &= t_0 p_1 + t_1,\\
T_{m-1} &= t_0,
\end{aligned}$$

on aura cette valeur de $\psi(x_1)$,

$$(17)\quad \psi(x_1) = \frac{T_{m-1} y_1^{m-1} + T_{m-2} y_1^{m-2} + \ldots + T_1 y_1 T_0}{m y_1^{m-1} + (m-1) p_1 y_1^{m-2} + \ldots + 2 p_{m-2} y_1 + p_{m-1}}.$$

La formule précédente n'est en défaut que si le dénominateur du second membre est nul. Or je dis qu'on peut toujours faire en sorte que cela ne soit pas. En effet, ce dénominateur est égal au produit

$$(y_1 - y_2)(y_1 - y_3) . \quad (y_1 - y_m),$$

et pour qu'il soit nul, il faudrait que l'un des facteurs le fût, que l'on eût, par exemple,

$$y_1 = y_k.$$

Cela posé, prenons pour y_1 la fonction

$$y_1 = (\alpha - x_1)(\alpha - \theta x_1)(\alpha - \theta^2 x_1) \ldots (\alpha - \theta^{n-1} x\ ),$$

α étant indéterminé; l'équation $y_1 = y_k$, ou

$$(\alpha - x_1)(\alpha - \theta x_1) \ldots = (\alpha - x_k)(\alpha - \theta x_k) \ldots,$$

ne peut avoir lieu, quel que soit α, à moins d'être identique; ce qui est impossible, puisque les quantités x_k, θx_k, etc., sont différentes de x_1, θx_1, etc. D'où il suit qu'en choisissant y_1 comme il vient d'être dit, l'équation (17) donnera pour $\psi(x_1)$ une valeur déterminée.

Les coefficients A'_1, A'_2, etc., de l'équation (8), peuvent donc s'exprimer rationnellement par une même fonction

y_1 dont la valeur dépend d'une équation du degré m; et si dans ces coefficients on remplace y_1 successivement par $y_2, y_3, \ldots, y_m$, on aura m équations du degré n, dont les racines seront respectivement

$$\begin{array}{l} x_1,\ \theta x_1, \ldots,\ \theta^{n-1} x_1, \\ x_2,\ \theta x_2, \ldots,\ \theta^{n-1} x_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x_m,\ \theta x_m, \ldots,\ \theta^{n-1} x_m. \end{array}$$

D'où il suit que l'équation proposée peut être décomposée en m équations chacune du degré n, dont les coefficients sont respectivement des fonctions rationnelles d'une même racine d'une équation du degré m.

Cette dernière équation n'est pas en général résoluble algébriquement, quand son degré surpasse le quatrième; mais l'équation (8) et les autres semblables le sont toujours, en supposant connus les coefficients A'_1, A''_1, etc., comme nous le démontrerons dans la leçon suivante.

VINGT-SEPTIÈME LEÇON.

Résolution algébrique des équations dont toutes les racines peuvent être représentées par $x, \theta x, \theta^2 x, \ldots, \theta^{\mu-1} x$, θx étant une fonction rationnelle de x et de quantités connues, telle que $\theta^{\mu} x = x$. — Cas où les quantités connues de f et de θ sont réelles. — Simplification pour les équations dont le degré est un nombre composé.

D'après la théorie exposée dans la leçon précédente, si deux racines d'une équation irréductible de degré $\mu = mn$ sont telles, que l'on puisse exprimer rationnellement l'une par l'autre, l'équation se décompose en m équations du degré n dont les racines peuvent être représentées par

$$x,\ \theta x,\ \theta^2 x, \ldots,\ \theta^{n-1} x,$$

et dont les coefficients sont des fonctions rationnelles respectivement d'une même racine d'une équation de degré m.

Si l'on a $m = 1$, et par suite $\mu = n$, ce qui arrive nécessairement dans le cas de μ premier, les μ racines de l'équation proposée sont représentées par

$$x,\ \theta x,\ \theta^2 x, \ldots,\ \theta^{\mu-1} x,$$

θx désignant une fonction rationnelle de x et de quantités connues, telle que

$$\theta^{\mu} x = x.$$

Toute équation qui a cette propriété peut être résolue algébriquement : la démonstration de cet important théorème va faire le sujet de cette leçon.

Résolution algébrique des équations dont toutes les racines peuvent être représentées par $x, \theta x, \theta^2 x, \ldots, \theta^{\mu-1} x$.

Soit

$$f(x) = 0 \tag{1}$$

une équation de degré μ, dont les racines sont

$$x,\ \theta x,\ \theta^2 x, \ldots,\ \theta^{\mu-1} x,$$

θx désignant une fonction rationnelle de x et de quantités connues, telle que

$$\theta^{\mu} x = x, \tag{2}$$

et, par conséquent,

$$\theta^{\mu+k} x = \theta^k x. \tag{3}$$

Désignons par α une racine quelconque de

$$x^{\mu} = 1,$$

et posons, avec Lagrange,

$$\psi(x) = \left(x + \alpha\theta x + \alpha^2\theta^2 x + \ldots + \alpha^{\mu-1}\theta^{\mu-1} x\right)^{\mu}; \tag{4}$$

je dis que la fonction $\psi(x)$ est exprimable rationnellement par les coefficients de $f(x)$ et de $\theta(x)$.

En effet, remplaçons x par $\theta^m x$, dans l'équation (4), on aura

$$\psi(\theta^m x) = \left(\theta^m x + \alpha\theta^{m+1} x + \alpha^2\theta^{m+2} x + \ldots + \alpha^{\mu-1}\theta^{m+\mu-1}\right)^{\mu},$$

et, en ayant égard aux équations (2) et (3),

$$\begin{aligned}\psi(\theta^m x) &= \left(\theta^m x + \alpha\theta^{m+1} x + \ldots + \alpha^{\mu-m} x + \alpha^{\mu-m+1}\theta x + \ldots + \alpha^{\mu-1}\theta^{m-1} x\right)^{\mu} \\ &= \left(\alpha^{\mu-m} x + \alpha^{\mu-m+1}\theta x + \ldots + \alpha^{\mu-1}\theta^{m-1} x + \theta^m x + \ldots + \alpha^{\mu-m-1}\theta\right)^{\mu} \\ &= \left(\alpha^{\mu-m}\right)^{\mu}\left(x + \alpha\theta x + \alpha^2\theta^2 x + \ldots + \alpha^{\mu-1}\theta^{\mu-1} x\right)^{\mu},\end{aligned}$$

ou enfin, à cause de $\alpha^\mu = 1$,

$$\psi(\theta^m x) = \psi(x).$$

Donnant à m les valeurs successives $0, 1, 2, \ldots, \mu-1$, on a

$$\psi(x) = \psi(\theta x) = \psi(\theta^2 x) = \ldots = \psi\left(\theta^{\mu-1} x\right),$$

et, par conséquent,

$$\psi(x) = \frac{1}{\mu}\left[\psi(x) + \psi(\theta x) + \ldots + \psi\left(\theta^{\mu-1} x\right)\right];$$

d'où il suit que $\psi(x)$ est une fonction rationnelle et symétrique de toutes les racines de l'équation (1); elle pourra donc être exprimée rationnellement par les coefficients de cette équation.

Posons alors

$$\psi(x) = v,$$

on aura

$$x + \alpha\theta x + \alpha^2\theta^2 x + \ldots + \alpha^{\mu-1}\theta^{\mu-1} x = \sqrt[\mu]{v},$$

v étant une quantité connue. Et si l'on désigne par

$$1,\ \alpha_1,\ \alpha_2,\ \ldots,\ \alpha_{\mu-1}$$

les μ racines de l'équation

$$x^\mu = 1,$$

par

$$v_0,\ v_1,\ v_2,\ \ldots,\ v_{\mu-1}$$

les valeurs correspondantes de v, on aura

$$(5)\quad \begin{cases} x + \theta x + \theta^2 x + \ldots\ldots\ldots\ldots\ldots + \theta^{\mu-1} x = \sqrt[\mu]{v_0}, \\ x + \alpha_1\theta x + \alpha_1^2\theta^2 x + \ldots\ldots + \alpha_1^{\mu-1}\theta^{\mu-1} x = \sqrt[\mu]{v_1}, \\ x + \alpha_2\theta x + \alpha_2^2\theta^2 x + \ldots\ldots + \alpha_2^{\mu-1}\theta^{\mu-1} x = \sqrt[\mu]{v_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x + \alpha_{\mu-1}\theta x + \alpha_{\mu-1}^2\theta^2 x + \ldots + \alpha_{\mu-1}^{\mu-1}\theta^{\mu-1} x = \sqrt[\mu]{v_{\mu-1}}. \end{cases}$$

La quantité $\sqrt[\mu]{v_0}$ est immédiatement donnée par l'équation (1); car si l'on désigne par A le coefficient de $x^{\mu-1}$ dans cette équation, on a

$$\sqrt[\mu]{v_0} = -A.$$

En ajoutant les équations (5), et ayant égard aux propriétés connues des racines α, on a

$$(6)\qquad x = \frac{-A + \sqrt[\mu]{v_1} + \sqrt[\mu]{v_2} + \ldots + \sqrt[\mu]{v_{\mu-1}}}{\mu};$$

et l'on aura généralement la valeur d'une racine quelconque $\theta^m x$, en ajoutant les équations (5) respectivement multipliées par

$$1,\ \alpha_1^{-m},\ \alpha_2^{-m},\ \alpha_3^{-m},\ldots,\ \alpha_{\mu-1}^{-m};$$

on trouve ainsi

$$(7)\quad \theta^m x = \frac{-A + \alpha_1^{-m}\sqrt[\mu]{v_1} + \alpha_2^{-m}\sqrt[\mu]{v_2} + \ldots + \alpha_{\mu-1}^{-m}\sqrt[\mu]{v_{\mu-1}}}{\mu},$$

et l'on déduira de cette formule les valeurs de θx, $\theta^2 x,\ldots,$ $\theta^{\mu-1}x$, en donnant à m les valeurs $1, 2, 3,\ldots, (m-1)$.

Dans l'équation (6) et dans toutes celles qu'on déduit de l'équation (7), on doit considérer chaque radical $\sqrt[\mu]{v_1}$, $\sqrt[\mu]{v_2},\ldots,$ $\sqrt[\mu]{v_{\mu-1}}$, comme ayant toujours la même valeur. Si on laisse à chaque radical toute sa généralité, l'équation (7) ne diffère aucunement de l'équation (6), et cette dernière renferme l'expression de toutes les racines. Il y a même ici une difficulté, car l'équation (6) donne pour x une expression qui a $\mu^{\mu-1}$ valeurs, tandis

que l'équation (1) n'a que μ racines. Mais nous avons déjà eu l'occasion d'indiquer comment on peut faire disparaître cette ambiguïté, en remarquant que quand on a fixé la valeur de l'un des radicaux, les autres sont par cela même déterminés.

Désignons par α une racine primitive de l'équation

$$x^\mu = 1,$$

et posons

$$\alpha_1 = \alpha,\quad \alpha_2 = \alpha^2,\quad \alpha_3 = \alpha^3,\ \ldots,\ \alpha_{\mu-1} = \alpha^{\mu-1},$$

on aura

$$\sqrt[\mu]{v_1} = x + \alpha\theta x + \alpha^2\theta^2 x + \ldots + \alpha^{\mu-1}\theta^{\mu-1}x,$$

$$\sqrt[\mu]{v_n} = x + \alpha^n\theta x + \alpha^{2n}\theta^2 x + \ldots + \alpha^{(\mu-1)n}\theta^{\mu-1}x.$$

Si l'on change x en $\theta^m x$, $\sqrt[\mu]{v_1}$ n'éprouve d'autre changement que d'être multiplié par $\alpha^{\mu-m}$; cela résulte immédiatement d'un calcul fait au commencement de cette leçon. Pareillement $\sqrt[\mu]{v_n}$ sera, par le même changement de x en $\theta^m x$, multiplié par $\alpha^{n(\mu-m)}$; d'où il suit que le produit

$$\sqrt[\mu]{v_n}\left(\sqrt[\mu]{v_1}\right)^{\mu-n}$$

sera multiplié par $\alpha^{\mu(\mu-m)} = 1$, c'est-à-dire qu'il n'éprouvera aucun changement. Si donc on pose

$$\sqrt[\mu]{v_n}\left(\sqrt[\mu]{v_1}\right)^{\mu-n} = \varphi(x),$$

on aura

$$\varphi(x) = \varphi(\theta x) = \varphi(\theta^2 x) = \ldots = \varphi(\theta^{\mu-1}x),$$

et, par conséquent,

$$\varphi(x) = \frac{1}{\mu}\left[\varphi(x) + \varphi(\theta x) + \ldots + \varphi\left(\theta^{\mu-1} x\right)\right].$$

$\varphi(x)$ est donc une fonction rationnelle et symétrique des racines de l'équation (1), et on pourra l'exprimer rationnellement par les quantités connues; en désignant par a_n sa valeur, on aura

$$\sqrt[\mu]{v_n}\left(\sqrt[\mu]{v_1}\right)^{\mu-n} = a_n,$$

ou

$$\sqrt[\mu]{v_n} = \frac{a_n}{v_1}\left(\sqrt[\mu]{v_1}\right)^n.$$

On pourra de cette manière exprimer chacun des radicaux $\sqrt[\mu]{v_2}$, $\sqrt[\mu]{v_3}$, etc., en fonction rationnelle de $\sqrt[\mu]{v_1}$, et l'équation (6) prendra la forme

$$(8)\quad x = \frac{1}{\mu}\left[-A + \sqrt[\mu]{v_1} + \frac{a_2}{v_1}\left(\sqrt[\mu]{v_1}\right)^2 + \frac{a_3}{v_1}\left(\sqrt[\mu]{v_1}\right)^3 + \ldots + \frac{a_{\mu-1}}{v_1}\left(\sqrt[\mu]{v_1}\right)^{\mu-1}\right].$$

Cette expression de x a précisément μ valeurs, et représente bien les μ racines de l'équation proposée.

Il résulte de ce qui précède que *si les μ racines d'une équation quelconque peuvent être représentées par*

$$x,\ \theta x,\ \theta^2 x, \ldots,\ \theta^{\mu-1} x,$$

θx étant une fonction rationnelle telle que $\theta^\mu = x$, l'équation est toujours soluble par radicaux, ainsi que nous l'avions annoncé.

Et en rapprochant cet énoncé du théorème démontré dans la dernière leçon, on a cet autre théorème :

Si deux racines d'une équation irréductible de degré premier sont telles, que l'une puisse s'exprimer rationnel-

lement en fonction de l'autre, l'équation est soluble par radicaux.

Cas où les quantités connues de f et de θ sont réelles.

Si tous les coefficients de f et de θ sont réels, on a un théorème remarquable, que M. Gauss a établi le premier pour les équations dont dépend la division du cercle en parties égales.

Nous avons posé précédemment

$$v_1 = \left(x + \alpha\theta x + \alpha^2\theta^2 x + \ldots + \alpha^{\mu-1}\theta^{\mu-1} x\right)^{\mu},$$

et nous avons établi que v_1 est une fonction symétrique des racines de l'équation $f(x) = 0$, par conséquent v_1 est exprimable rationnellement par les coefficients de f et de θ; et si ces quantités sont toutes réelles, v_1 ne contiendra d'autres imaginaires que celle de la racine α. En outre, $v_{\mu-1}$ se déduit de v_1 en remplaçant α par l'expression conjuguée $\alpha^{\mu-1}$; d'où il résulte que v_1 et $v_{\mu-1}$ sont des quantités connues imaginaires et conjuguées. On pourra donc poser

$$(9) \qquad \begin{cases} v_1 = \rho(\cos\omega + \sqrt{-1}\sin\omega), \\ v_{\mu-1} = \rho(\cos\omega - \sqrt{-1}\sin\omega). \end{cases}$$

Nous avons aussi, en général,

$$\left(\sqrt[\mu]{v_1}\right)^{\mu-1}\sqrt[\mu]{v_n} = a_n,$$

et, pour $n = \mu - 1$,

$$(10) \qquad \sqrt[\mu]{v_1}\sqrt[\mu]{v_{\mu-1}} = a_{\mu-1}.$$

$a_{\mu-1}$ est exprimable rationnellement par les coefficients de f et de θ, elle ne peut donc renfermer d'autres ima-

ginaires que celle qui se trouve dans α. Mais il est évident que $a_{\mu-1}$ ne change pas si l'on remplace α par $\alpha^{\nu-1}$ qui est sa conjuguée; donc $a_{\mu-1}$ est réelle.

Des équations (9) et (10) on déduit

$$\rho^2 = a_{\mu-1}^{\mu},$$

et, en désignant par a la valeur numérique de $a_{\mu-1}$

$$\sqrt[\mu]{\rho} = \sqrt{a}.$$

La première des équations (9) donne alors cette valeur de $\sqrt[\mu]{\nu_1}$,

$$\sqrt[\mu]{\nu_1} = \sqrt{a}\left(\cos\frac{\omega + 2k\pi}{\mu} + \sqrt{-1}\sin\frac{\omega + 2k\pi}{\mu}\right),$$

et l'expression des racines x, donnée par l'équation (8), prend cette forme très-remarquable

$$x = \frac{1}{\mu}\left\{\begin{array}{l} -A + \sqrt{a}\left(\cos\frac{\omega + 2k\pi}{\mu} + \sqrt{-1}\sin\omega + 2k\pi\right) \\ +(f+g\sqrt{-1})\left(\cos 2\frac{\omega+2k\pi}{\mu} + \sqrt{-1}\sin 2\frac{\omega+2k\pi}{\mu}\right) \\ +(F+G\sqrt{-1})\sqrt{a}\left(\cos 3\frac{\omega+2k\pi}{\mu} + \sqrt{-1}\sin 3\frac{\omega+2k\pi}{\mu}\right) \\ +(f_1+g_1\sqrt{-1})\left(\cos 4\frac{\omega+2k\pi}{\mu} + \sqrt{-1}\sin 4\frac{\omega+2k\pi}{\mu}\right) \\ +\ldots \end{array}\right\},$$

où a, f, g, F, G, f_1, g_1, etc., sont des fonctions rationnelles de $\cos\frac{2\pi}{\mu}$ et de $\sin\frac{2\pi}{\mu}$.

L'équation précédente fera connaître les μ racines de $f(x) = 0$, en donnant au nombre entier k les μ valeurs $0, 1, 2, 3, \ldots, \mu - 1$. De là résulte le théorème suivant.

THÉORÈME. — *Pour résoudre l'équation* (1) $f(x) = 0$, *il suffit :*

1° *De diviser la circonférence entière du cercle en* μ *parties égales; 2° de diviser ensuite un angle* ω *en* μ *parties égales; 3° d'extraire la racine carrée d'une seule quantité* a.

REMARQUE. — Les coefficients de f et de θ étant tous réels, si une racine de $f(x) = 0$ est réelle, toutes les autres le seront; puisque, si x désigne cette racine réelle, les autres racines sont

$$\theta x, \ \theta^2 x, \ldots, \ \theta^{\mu-1} x.$$

Par conséquent, l'équation proposée a ses racines ou toutes réelles, ou toutes imaginaires.

Simplification pour le cas où le degré μ *est un nombre composé.*

La méthode qui vient d'être exposée pour la résolution algébrique de l'équation

$$(1) \qquad f(x) = 0$$

est applicable à tous les cas, que μ soit premier ou non; mais, dans ce dernier cas, on peut simplifier la solution.

Soit $\mu = mn$. Les racines de l'équation (1) étant toujours

$$x, \ \theta x, \ \theta^2 x, \ldots, \ \theta^{\mu-1} x,$$

nous pourrons les partager en m groupes de la manière suivante :

$$(2) \quad \left\{ \begin{array}{l} x, \ \theta^m x, \ \theta^{2m} x, \ldots, \ \theta^{(n-1)m} x, \\ \theta x, \ \theta^{m+1} x, \ \theta^{2m+1} x, \ldots, \ \theta^{(n-1)m+1} x, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \theta^{m-1} x, \ \theta^{2m-1} x, \ \theta^{3m-1} x, \ldots, \ \theta^{nm-1} x; \end{array} \right.$$

ou, en posant,

$$x = x_1, \quad \theta x = x_2, \quad \theta^2 x = x_3, \ldots, \quad \theta^{m-1} x = x_m,$$

et

$$\theta^m x = \theta_1 x,$$

de la manière suivante :

$$(2) \quad \begin{cases} x_1, \ \theta_1 x_1, \ \theta_1^2 x_1, \ldots, \ \theta_1^{n-1} x_1, \\ x_2, \ \theta_1 x_2, \ \theta_1^2 x_2, \ldots, \ \theta_1^{n-1} x_2, \\ \ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots \\ x_m, \ \theta_1 x_m, \ \theta_1^2 x_m, \ldots, \ \theta_1^{n-1} x_m. \end{cases}$$

En appliquant donc à l'équation (1) la méthode exposée dans la leçon précédente, on pourra la décomposer en m équations, chacune du degré n, qui auront respectivement pour racines les divers groupes (2), et dont les coefficients seront des fonctions rationnelles d'une même racine d'une équation

$$(3) \qquad \psi(y) = 0$$

de degré m. Soient

$$y_1, \ y_2, \ldots, \ y_m,$$

les m racines de l'équation (3), et

$$(4) \qquad \varphi(x, y_1) = 0, \quad \varphi(x, y_2) = 0, \ldots, \ \varphi(x, y_m) = 0$$

les m équations qui ont respectivement pour racines les quantités du premier groupe (2), du deuxième, etc., du dernier. Je dis que, pour résoudre l'équation (1), il suffit de connaître une racine y de l'équation (3), et ensuite une racine x de l'équation

$$(5) \qquad \varphi(x, y) = 0$$

correspondante ; car on aura, de cette manière, une racine x de l'équation (1), et les autres seront

$$\theta x, \ \theta^2 x, \ldots, \ \theta^{\mu-1} x.$$

L'équation proposée (1) étant résoluble algébriquement, l'équation (3) l'est aussi; car y désigne une fonction rationnelle de x. Mais je dis de plus que l'équation (3) jouit de la même propriété que l'équation (1), et que, par conséquent, on pourra lui appliquer la méthode de résolution précédemment exposée.

En effet, les racines de l'équation (1), renfermées dans le premier des groupes (2), sont

$$(6) \qquad x,\ \theta^m x,\ \theta^{2m} x, \ldots,\ \theta^{(n-1)m} x,$$

et y désigne une fonction rationnelle et symétrique de ces racines, c'est-à-dire une fonction rationnelle de x. Posons

$$y = \mathrm{F}(x,\ \theta^m x,\ \theta^{2m} x, \ldots,\ \theta^{(n-1)m} x) = \mathrm{F}(x),$$

les m racines $y_1, y_2, \ldots, y_m$ de l'équation (3) seront

$$\mathrm{F}(x),\ \mathrm{F}(\theta x),\ \mathrm{F}(\theta^2 x), \ldots,\ \mathrm{F}(\theta^{m-1} x),$$

et l'on aura

$$\mathrm{F}(\theta x) = \mathrm{F}(\theta x,\ \theta\theta^m x,\ \theta\theta^{2m} x, \ldots,\ \theta\theta^{(n-1)m} x).$$

Par conséquent, $\mathrm{F}(\theta x)$ et $\mathrm{F}(x)$ sont des fonctions rationnelles et symétriques des quantités (6), et l'on pourra exprimer rationnellement l'une par l'autre par la méthode des fonctions semblables rappelée dans la dernière leçon.

Soit donc

$$\mathrm{F}(\theta x) = \lambda \mathrm{F}(x) = \lambda y,$$

λx étant une fonction rationnelle de x, on aura

$$\mathrm{F}(\theta^2 x) = \lambda \mathrm{F}(\theta x) = \lambda^2 y,$$
$$\mathrm{F}(\theta^3 x) = \lambda \mathrm{F}(\theta^2 x) = \lambda^3 y,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\mathrm{F}(\theta^{m-1} x) = \lambda \mathrm{F}(\theta^{m-2} x) = \lambda^{m-1} y,$$

et l'on voit que les m racines de l'équation (3) pourront

être représentées par

$$y, \lambda y, \lambda^2 y, \ldots, \lambda^{m-1} y,$$

λ désignant une fonction rationnelle telle que $\lambda^m y = y$.

L'équation (3) une fois résolue, y sera connu, et on pourra appliquer à l'équation (5) la méthode précédemment exposée, puisque ses n racines peuvent être représentées par

$$x, \theta_1 x, \theta_1^2 x, \ldots, \theta_1^{n-1} x.$$

On peut donc énoncer le théorème suivant :

Si $\mu = mn$, la résolution de l'équation (1) *est ramenée à celle de deux équations des degrés m et n respectivement, et qui ont la même propriété que la proposée.*

Si n est lui-même un nombre composé $m_1 n_1$, on ramènera, de la même manière, la résolution de l'équation (5) à celle d'une équation en z

$$(7) \qquad \psi_1(z, y) = 0$$

de degré m_1, et à celle d'une équation en x de degré n_1

$$(8) \qquad \varphi_1(x, y, z) = 0.$$

Dans l'équation (7), y fait partie des quantités connues, et dans l'équation (8) il en est de même de y et de z, et, généralement, on a ce théorème :

Théorème. — *Si $\mu = m_1 m_2 \ldots m_n$, la résolution de l'équation* (1) *est ramenée à celle de n équations des degrés*

$$m_1, m_2, \ldots, m_n,$$

respectivement, et il suffit même de connaître une racine de chacune de ces équations, qui ont toutes la même propriété que l'équation proposée.

Corollaire. — *Si, en décomposant μ en facteurs pre-*

miers, on a

$$\mu = \varepsilon_1^{p_1} \varepsilon_2^{p_2} \ldots \varepsilon_\omega^{p_\omega},$$

la résolution de l'équation proposée de degré μ se ramènera à celle de p_1 équations du degré ε_1, de p_2 équations du degré $\varepsilon_2, \ldots,$ de p_ω équations du degré ε_ω.

Exemple. — Supposons que $\mu = 30$, les racines de

$$(1) \qquad f(x) = 0$$

seront

$$x,\ \theta x,\ \theta^2 x, \ldots,\ \theta^{29} x.$$

Comme $30 = 2 \times 15$, on prendra pour y une fonction rationnelle et symétrique des quinze racines

$$x,\ \theta^2 x,\ \theta^4 x, \ldots,\ \theta^{28} x;$$

y dépendra d'une équation du second degré

$$(2) \qquad y^2 + Ay + B = 0,$$

dont les coefficients seront immédiatement exprimables par ceux de la proposée; on pourrait former ensuite l'équation du quinzième degré ayant pour racines x, $\theta^2 x, \ldots, \theta^{28} x$, mais il est inutile de faire ce calcul : représentons, comme précédemment, par

$$\varphi(x, y) = 0$$

cette équation, où y est une quantité connue. Comme $15 = 3 \times 5$, on prendra pour z une fonction rationnelle et symétrique des cinq racines

$$x,\ \theta^6 x,\ \theta^{12} x,\ \theta^{18} x,\ \theta^{24} x;$$

z dépendra d'une équation du troisième degré

$$(3) \qquad z^3 + Cz^2 + Dz + E = 0,$$

dont les coefficients seront des fonctions rationnelles de y et des autres quantités connues; enfin on formera l'équation

$$(4)\qquad x^5 + Fx^4 + Gx^3 + Hx^2 + Kx + L = 0,$$

ayant pour racines

$$x,\ \theta^6 x,\ \theta^{12} x,\ \theta^{18} x,\ \theta^{24} x,$$

et dont les coefficients seront fonctions rationnelles de y et de z. La résolution de l'équation (1) sera ainsi ramenée à trouver une racine de l'équation (2), puis une de l'équation (3), puis enfin une de l'équation (4).

Autre manière de ramener la résolution de l'équation (1) *à celle d'équations de degrés inférieurs.*

Revenons au cas général, et supposons

$$\mu = m_1 m_2 \ldots m_\omega.$$

Désignons par $n_1, n_2, \ldots, n_\omega$ les quotients respectifs de μ par $m_1, m_2, \ldots, m_\omega$, on aura

$$\mu = m_1 n_1 = m_2 n_2 = m_3 n_3 = \ldots = m_\omega n_\omega.$$

Cela posé, on peut, d'après ce qui précède, décomposer l'équation

$$f(x) = 0$$

en deux équations, des ω manières suivantes :

(1) $\varphi_1(x, y_1) = 0$ ayant pour racines $x,\ \theta^{m_1} x,\ \theta^{2m_1} x, \ldots,$ $\theta^{(n_1-1)m_1} x$, et dont les coefficients sont des fonctions rationnelles d'une racine y_1 d'une équation $\psi_1(y_1) = 0$ de degré m_1.

(2) $\varphi_2(x, y_2) = 0$ ayant pour racines x, $\theta^{m_2}x$, $\theta^{2m_2}x, \ldots$, $\theta^{(n_2-1)m_2}x$, et dont les coefficients sont des fonctions rationnelles d'une racine y_2 d'une équation $\psi_2(y_2) = 0$ de degré m_2.

. . . .

. . . .

(ω) $\varphi_\omega(x, y_\omega) = 0$ ayant pour racines x, $\theta^{m_\omega}x$, $\theta^{2m_\omega}x, \ldots$, $\theta^{(n_\omega-1)m_\omega}x$, et dont les coefficients sont des fonctions rationnelles d'une racine y_ω d'une équation $\psi_\omega(y_\omega) = 0$ de degré m_ω.

Supposons maintenant que $m_1, m_2, \ldots, m_\omega$ soient premiers entre eux, les équations

$$\varphi_1(x, y_1) = 0, \quad \varphi_2(x, y_2) = 0, \ldots, \varphi_\omega(x, y_\omega) = 0$$

n'auront que la seule racine x commune; donc, suivant un théorème connu, on peut exprimer x rationnellement par les coefficients de ces équations, et, par conséquent, en fonction rationnelle de $y_1, y_2, \ldots, y_\omega$. Ces dernières quantités étant connues, on aura une racine de l'équation (1), et, par suite, toutes les racines.

La résolution de l'équation (1) est donc ramenée à trouver une racine de chacune des équations

$$\psi_1(y_1) = 0, \quad \psi_2(y_2) = 0, \ldots, \psi_\omega(y_\omega) = 0,$$

qui sont respectivement des degrés $m_1, m_2, \ldots, m_\omega$. En outre, ces équations ont la même propriété que la proposée, ainsi que nous l'avons établi précédemment; on pourra donc leur appliquer la même méthode. Si l'on veut que ces équations soient les moins élevées possibles, et si, en décomposant μ en facteurs premiers, on a

$$\mu = \varepsilon_1^{p_1} \varepsilon_2^{p_2} \ldots \varepsilon_\omega^{p_\omega},$$

il faudra prendre

$$m_1 = \varepsilon_1^{p_1}, \ m_2 = \varepsilon_2^{p_2}, \ldots, m_\omega = \varepsilon_\omega^{p_\omega},$$

Quant à la résolution de chacune des équations

$$\psi(y) = 0$$

de degré ε^p, elle se ramènera à celle de p équations de degré ε, ainsi que nous l'avons démontré.

Corollaire. — *Toute équation de degré 2^p, dont les racines peuvent être représentées par*

$$x, \ \theta x, \ \theta^2 x, \ldots, \theta^{2^p} x,$$

peut être résolue à l'aide de p extractions de racines carrées.

VINGT-HUITIÈME LEÇON.

Résolution algébrique des équations dont dépend la division du cercle en un nombre premier de parties égales. — Division de la circonférence en dix-sept parties égales. — Construction géometrique.

Résolution algébrique des équations dont dépend la division du cercle en un nombre premier de parties égales.

Le problème de la division du cercle en un nombre m quelconque de parties égales se ramène à la résolution de l'équation binôme

$$z^m - 1 = 0; \tag{1}$$

car, si l'on fait

$$\frac{2\pi}{m} = k,$$

on obtiendra les m racines de l'équation précédente, en donnant à k les m valeurs

$$0,\ 1,\ 2,\ 3, \ldots (m-1)$$

dans la formule

$$z = \cos ka + \sqrt{-1}\sin ka;$$

on connaîtra donc $\cos ka$ et $\sin ka$ lorsque l'équation binôme sera résolue algébriquement.

Nous avons vu, dans la treizième leçon, que si m est un nombre composé, la résolution de l'équation (1) se ramène à celle d'équations de la même forme et de degré premier; nous supposerons donc m premier et égal à

$2\mu + 1$. En divisant l'équation (1) par $z - 1$, et posant ensuite

$$z + \frac{1}{z} = x,$$

elle devient (*voir* quatorzième leçon)

$$(2)\quad \left\{ \begin{aligned} & x^{\mu} + x^{\mu-1} - (\mu - 1) x^{\mu-2} - (\mu - 2) x^{\mu-3} \\ & \quad + \frac{(\mu-2)(\mu-3)}{1.2} x^{\mu-4} + \frac{(\mu-3)(\mu-4)}{1.2} x^{\mu-5} - \text{etc.} = 0. \end{aligned} \right.$$

C'est de cette équation (2) que dépend directement la division du cercle en $2\mu + 1$ parties égales. Ses μ racines sont représentées par la formule

$$x = 2 \cos \frac{2k\pi}{2\mu + 1} = 2 \cos k a,$$

dans laquelle on doit donner à k les μ valeurs

$$1,\ 2,\ 3,\ \ldots\ \mu,$$

ou des valeurs qui n'en diffèrent que par des multiples de $2\mu + 1$.

Soit n une racine primitive pour le nombre premier $2\mu + 1$; je dis que les μ racines de l'équation (2) seront

$$(3)\qquad 2\cos a,\quad 2\cos na,\quad 2\cos n^2 a,\ \ldots,\ 2\cos n^{\mu-1} a.$$

Il est évident que chacune de ces μ quantités satisfait à l'équation (2); il suffit donc de démontrer qu'elles sont toutes distinctes. Supposons, s'il est possible, que deux de ces quantités soient égales, et que l'on ait

$$2\cos n^p a = 2\cos n^q a,$$

p et q étant $< \mu$; on aurait

$$n^p a \pm n^q a = 2\lambda\pi,$$

λ désignant un nombre entier. Mais $a = \frac{2\pi}{2\mu + 1}$, donc

$$\frac{n^q(n^{p-q} \pm 1)}{2\mu + 1}$$

serait un nombre entier; et comme $2\mu + 1$ est premier, et que $n < 2\mu + 1$, il s'ensuit que $2\mu + 1$ diviserait l'un des deux nombres $n^{p-q} + 1$ ou $n^{p-q} - 1$; il diviserait donc leur produit

$$n^{2p-2q} - 1:$$

or ceci est impossible, car $2p - 2q$ est $< 2\mu$, et n désigne une racine primitive de $2\mu + 1$. Donc les quantités (3) sont bien toutes les racines de l'équation (2).

Si maintenant on fait

$$x = 2\cos a, \qquad \theta x = 2\cos na,$$

on aura

$$\theta^2 x = 2\cos n^2 a, \quad \theta^3 x = 2\cos n^3 a, \ldots, \theta^{\mu-1} x = 2\cos n^{\mu-1} a,$$

et les racines de l'équation (2) seront représentées par

$$x, \quad \theta x, \quad \theta^2 x, \; \ldots \; \theta^{\mu-1} x;$$

on a, en outre, $\theta^{\mu} x = x$; car n étant racine primitive de $2\mu + 1$, on a $n^{\mu} \equiv -1 \pmod{2\mu + 1}$; enfin θx est une fonction rationnelle de x, car $\cos na$ est exprimable rationnellement en fonction de $\cos a$. On voit donc que l'équation (2) est comprise dans la classe d'équations que nous avons étudiée dans la dernière leçon, et l'on pourra la résoudre par la méthode que nous avons exposée.

Ici, la fonction rationnelle θx a pour valeur (*voir* quatorzième leçon)

$$\theta x = x^n + x^{n-1} - (n-1)x^{n-2} - (n-2)x^{n-3} + \frac{(n-2)(n-3)}{1.2} x^{n-4} + \text{etc.}$$

En appliquant à l'équation (2) les théorèmes de la leçon précédente, on obtient les énoncés suivants :

1°. *Si $\mu = m_1 m_2 \ldots m_\omega$, on peut diviser la circonférence entière du cercle en $2\mu + 1$ parties égales à l'aide de ω équations des degrés $m_1, m_2, \ldots, m_\omega$ respectivement. Si les nombres $m_1, m_2, \ldots, m_\omega$ sont premiers entre eux, les coefficients de ces équations seront des nombres rationnels.*

2°. *Si $\mu = 2^\omega$, on pourra diviser la circonférence du cercle en $2\mu + 1$ parties égales, à l'aide de ω racines carrées. En d'autres termes, si $2\mu + 1$ est un nombre premier, et $\mu = 2^\omega$, on pourra diviser la circonférence du cercle en $2\mu + 1$ parties égales, avec la règle et le compas.*

3°. *Pour diviser la circonférence du cercle en $2\mu + 1$ parties égales, il suffit de diviser la circonférence entière en 2μ parties égales, de diviser un arc, qu'on peut construire ensuite en 2μ parties égales, et d'extraire la racine carrée d'une seule quantité*

Ce dernier théorème est dû à M. Gauss. Ce géomètre a prouvé, en outre, que la quantité dont il faut extraire la racine carrée est simplement le nombre entier $2\mu + 1$. Voici comment Abel le démontre :

En désignant par ρ cette quantité, ρ est, comme nous avons vu, la valeur numérique du produit

$$\left(x + \alpha\theta x + \alpha^2\theta^2 x + \ldots + \alpha^{\mu-1}\theta^{\mu-1} x\right)\left(x + \alpha^{\mu-1}\theta x + \alpha^{\mu-2}\theta^2 x + \ldots + \alpha\theta^{\mu-1} x\right),$$

où

$$\alpha = \cos\frac{2\pi}{\mu} + \sqrt{-1}\sin\frac{2\pi}{\mu}.$$

On a donc

$$\pm\rho = 4\left(\cos a + \alpha\cos na + \alpha^2\cos n^2 a + \ldots + \alpha^{\mu-1}\cos n^{\mu-1} a\right)$$
$$\times\left(\cos a + \alpha^{\mu-1}\cos na + \alpha^{\mu-2}\cos n^2 a + \ldots + \alpha\cos n^{\mu-1} a\right).$$

En développant ce produit, on aura un résultat de la forme

$$\pm \rho = t_0 + t_1\alpha + t_2\alpha^2 + \ldots + t_{\mu-1}\alpha^{\mu-1},$$

et l'on trouve facilement

$$t_m = 4\left(\cos a \cos n^m a + \cos na \cos n^{m+1} a + \ldots + \cos n^{\mu-1-m} a \cos n^{\mu-1} a\right)$$
$$+ 4\left(\cos n^{\mu-m} a \cos a + \cos n^{\mu-m+1} a \cos na + \ldots + \cos n^{\mu-1} a \cos n^{m-1} a\right).$$

En se servant de la formule

$$\cos n^p a \cos n^{m+p} a = \frac{1}{2}\cos(n^{m+p} a + n^p a) + \frac{1}{2}\cos(n^{m+p} a - n^p a),$$

la valeur de t_m prendra la forme

$$t_m = 2\left[\begin{array}{c}\cos(n^m+1)a + \cos(n^m+1)na + \cos(n^m+1)n^2 a + \ldots \\ + \cos(n^m+1)n^{\mu-1} a\end{array}\right]$$
$$+ 2\left[\begin{array}{c}\cos(n^m-1)a + \cos(n^m-1)na + \cos(n^m-1)n^2 a + \ldots \\ + \cos(n^m-1)n^{\mu-1} a\end{array}\right],$$

ou, en faisant

$$(n^m + 1)a = a', \quad (n^m - 1)a = a'',$$

$$t_m = 2\cos a' + \theta\, 2\cos a' + \theta^2\, 2\cos a' + \ldots + \theta^{\mu-1}\, 2\cos a'$$
$$+ 2\cos a'' + \theta\, 2\cos a'' + \theta^2 \cos a'' + \ldots + \theta^{\mu-1}\, 2\cos a''.$$

Cela posé, supposons d'abord que m ne soit pas nul; $2\cos a'$ et $2\cos a''$ sont des racines de l'équation (2), donc

$$2\cos a' = \theta^\delta x \quad \text{et} \quad 2\cos a'' = \theta^\varepsilon x,$$

et l'on aura

$$t_m = \left(\theta^\delta x + \theta^{\delta+1} x + \ldots + \theta^{\mu-1} x + x + \theta x + \ldots + \theta^{\delta-1} x\right)$$
$$+ \left(\theta^\varepsilon x + \theta^{\varepsilon+1} x + \ldots + \theta^{\mu-1} x + \theta x + \ldots\ldots + \theta^{\varepsilon-1} x\right),$$

ou

$$t_m = 2\left(x + \theta x + \theta^2 x + \ldots + \theta^{\mu-1} x\right);$$

c'est-à-dire que t_m est double de la somme des racines de l'équation (2), laquelle est égale à -1, on a donc

$$t_m = -2.$$

Supposons maintenant $m = 0$, on aura

$$t_0 = 2\left(\cos 2a + \cos 2na + \cos 2n^2 a + \ldots + \cos 2n^{\mu-1} a\right) + 2\mu.$$

Or $2\cos 2a$ est racine de l'équation (2); donc, en faisant

$$2\cos 2a = \theta^{\delta} x,$$

on aura

$$t_0 = \left(\theta^{\delta} x + \theta^{\delta+1} x + \ldots + \theta^{\mu-1} x + x + \theta x + \ldots + \theta^{\delta-1} x\right) + 2\mu,$$

et, par conséquent,

$$t_0 = 2\mu - 1.$$

D'après cela, la valeur de $\pm\rho$ sera

$$\pm\rho = 2\mu - 1 - 2\left(\alpha + \alpha^2 + \ldots + \alpha^{\mu-1}\right).$$

D'ailleurs

$$\alpha + \alpha^2 + \ldots + \alpha^{\mu-1} = -1,$$

donc

$$\pm\rho = 2\mu + 1.$$

Ce qu'il fallait démontrer.

Division de la circonférence en dix-sept parties égales.

En faisant $2\mu + 1 = 17$ ou $\mu = 8$, l'équation (2) du paragraphe précédent devient

$$(1)\quad x^8 + x^7 - 7x^6 - 6x^5 + 15x^4 - 10x^3 - 10x^2 - 4x + 1 = 0,$$

et ses racines, comprises dans la formule

$$x = 2\cos\frac{2k\pi}{17},$$

peuvent être représentées par

(2) $$x,\ \theta x,\ \theta^2 x,\ \theta^3 x,\ \theta^4 x,\ \theta^5 x,\ \theta^6 x,\ \theta^7 x.$$

La plus petite racine primitive de 17 est 3 (*voir* la Table des racines primitives, page 326), et les résidus par rapport à 17 des puissances

$$3^0,\ 3^1,\ 3^2,\ 3^3,\ 3^4,\ 3^5,\ 3^6,\ 3^7,$$

sont

$$1,\ 3,\ 9,\ 10,\ 13,\ 5,\ 15,\ 11;$$

donc, en faisant, pour abréger,

$$a = \frac{2\pi}{17},$$

les quantités (2) seront

$$2\cos a,\quad 2\cos 3a,\quad 2\cos 9a,\quad 2\cos 10a,$$
$$2\cos 13a,\quad 2\cos 5a,\quad 2\cos 15a,\quad 2\cos 11a.$$

Pour appliquer la méthode générale, il faut commencer par calculer une fonction rationnelle et symétrique y des quantités

$$2\cos a,\quad 2\cos 9a,\quad 2\cos 13a,\quad 2\cos 15a.$$

Posons donc

$$y = 2\cos a + 2\cos 9a + 2\cos 13a + 2\cos 15a,$$

y dépendra d'une équation du second degré, dont les deux racines seront

(3) $$y = 2\cos a + 2\cos 9a + 2\cos 13a + 2\cos 15a,$$

(4) $$y_1 = 2\cos 3a + 2\cos 10a + 2\cos 5a + 2\cos 11a.$$

Cette équation est bien aisée à former, car on a d'abord,

par l'équation (1),

$$y + y_1 = -1; \tag{5}$$

ensuite, en multipliant y par y_1 transformant les produits de cosinus en sommes à l'aide des formules connues, et ayant égard à l'équation identique

$$\cos(17 - m)a = \cos ma,$$

on trouve

$$yy_1 = 4\left(\begin{array}{c}2\cos a + 2\cos 13a + 2\cos 9a + 2\cos 10a + 2\cos 13a \\ +2\cos 5a + 2\cos 15a + 2\cos 11a\end{array}\right),$$

et, à cause de l'équation (1),

$$yy_1 = -4. \tag{6}$$

L'équation en y sera donc

$$y^2 + y - 4 = 0, \tag{7}$$

et l'on peut considérer comme connues ses deux racines y et y_1.

Maintenant les quantités

$$2\cos a, \quad 2\cos 9a, \quad 2\cos 13a, \quad 2\cos 15a$$

sont racines d'une équation du quatrième degré dont les coefficients sont fonctions rationnelles de y, et sur laquelle nous allons raisonner comme nous avons fait sur la proposée. Il faut, conformément à la méthode générale, chercher d'abord une fonction rationnelle et symétrique z des quantités

$$2\cos a, \quad 2\cos 13a.$$

Posons donc

$$z = 2\cos a + 2\cos 13a,$$

l'équation en z sera du second degré, et aura pour racines

$$z = 2\cos a + 2\cos 13a, \tag{8}$$

$$z_1 = 2\cos 9a + 2\cos 15a. \tag{9}$$

On a d'abord

(10) $$z + z_1 = y,$$

et en multipliant z par z_1, on trouve, après avoir remplacé les produits de cosinus par des sommes,

$$zz_1 = \begin{pmatrix} 2\cos a + 2\cos 3a + 2\cos 9a + 2\cos 10a + 2\cos 13a \\ + 2\cos 5a + 2\cos 15a + 2\cos 10a \end{pmatrix},$$

ou, à cause que la somme des racines de l'équation (1) est -1,

(11) $$zz_1 = -1;$$

l'équation en z sera donc

(12) $$z^2 - yz - 1 = 0.$$

Enfin il ne reste plus qu'à former l'équation du second degré dont les racines sont

$$2\cos a, \quad 2\cos 13a,$$

et dont les coefficients peuvent s'exprimer en fonction rationnelle de y et de z. Mais on peut simplifier ici l'application de la méthode générale.

Considérons l'équation du quatrième degré, dont les racines

$$2\cos 3a, \quad 2\cos 10a, \quad 2\cos 5a, \quad 2\cos 11a$$

ont pour somme y_1, et traitons-la comme nous avons fait de l'équation qui a pour racines les quantités dont la somme est y. On formera une équation du second degré ayant pour racines

(13) $$u = 2\cos 3a + 2\cos 5a,$$

(14) $$u_1 = 2\cos 10a + 2\cos 11a,$$

et, en opérant comme précédemment, on trouvera

(15) $$u + u_1 = y_1,$$

(16) $$uu_1 = -1;$$

cette équation en u sera donc

(17) $$u^2 - y_1 u - 1 = 0,$$

et les quantités u et u_1 sont connues, ainsi que z et z_1.

Cela posé, faisons

(18) $$x = 2\cos a,$$

(19) $$x_1 = 2\cos 13a,$$

on aura d'abord

(20) $$x + x_1 = z,$$

et ensuite

$$xx_1 = 4\cos a \cos 13a = 2\cos 14a + 2\cos 12a$$
$$= 2\cos 3a + 2\cos 5a$$

ou

(21) $$xx_1 = u;$$

x et x_1 seront donc racines de l'équation

(22) $$x^2 - zx + u = 0.$$

La résolution de l'équation (1) est ainsi ramenée à celle des équations du second degré (7), (12), (17) et (22); le problème est donc résolu. Nous allons chercher maintenant à déduire de la théorie précédente une construction géométrique, pour effectuer la division de la circonférence en dix-sept parties égales.

Construction géométrique.

Quand on se propose, dans la géométrie élémentaire, d'inscrire dans un cercle les polygones réguliers de trois ou de cinq côtés, on commence par inscrire ceux de six et de dix côtés. De même, nous commencerons ici par

inscrire le polygone régulier de trente-quatre côtés, celui de dix-sept côtés s'en déduira immédiatement.

Soit une demi-circonférence, *fig.* 3, partagée en dix-sept parties égales aux points

$$a,\ b,\ c,\ d,\ e,\ f,\ g,\ h,\ i,\ j,\ k,\ l,\ m,\ n,\ o,\ p,\ q,\ r;$$

la corde ab sera le côté du polygone régulier inscrit de trente-quatre côtés, et les cordes ad, af, ah, aj, al, an, ap seront les diagonales de ce polygone ou, si l'on veut, les côtés des polygones réguliers *étoilés* de trente-quatre côtés, que l'on peut inscrire dans la circonférence.

En prenant le rayon pour unité, et faisant, comme précédemment,

$$a = \frac{2\pi}{17},$$

on aura

$$ab = 2\sin\frac{\pi}{34} = +2\cos 13a,$$

$$ad = 2\sin\frac{3\pi}{34} = -2\cos 5a,$$

$$af = 2\sin\frac{5\pi}{34} = +2\cos 3a,$$

$$ah = 2\sin\frac{7\pi}{34} = -2\cos 11a,$$

$$aj = 2\sin\frac{9\pi}{34} = +2\cos 15a,$$

$$al = 2\sin\frac{11\pi}{34} = -2\cos 10a,$$

$$an = 2\sin\frac{13\pi}{34} = +2\cos a,$$

$$ap = 2\sin\frac{15\pi}{34} = -2\cos 9a.$$

Conservons toutes les notations du paragraphe précédent,

les équations (3) et (4) nous donnent

$$y = an - ap + ab + aj,$$
$$y_1 = af - al - ad - ah.$$

On voit que y_1 est négatif, car af est $< al$; par suite, y est positif, puisque $yy_1 = -1$. Faisant donc $y_1 = -y'$, les équations (5) et (6) deviennent

$$y' - y = 1,$$
$$yy' = 4.$$

Les équations (8) et (9) nous donnent

$$z = an + ab,$$
$$z_1 = -ap + aj;$$

z_1 est négatif, car ap est $> aj$, et z est positif. Les équations (10) et (11) deviennent, en faisant $z_1 = -z'$,

$$z - z' = y,$$
$$zz' = 1.$$

Pareillement, les équations (13) et (14) donnent

$$u = af - ad,$$
$$u_1 = -al - ah;$$

u_1 est donc négatif, et u positif. Faisant $u_1 = -u'$, on aura, par les équations (15) et (16),

$$u' - u = y',$$
$$uu' = 1;$$

enfin les équations (18) et (19) donnent

$$x = an,$$
$$x_1 = ab,$$

en sorte que x et x_1 sont positifs, et les équations (20)

et (21) conservent leur forme

$$x + x_1 = z,$$
$$xx_1 = u.$$

Le côté de notre polygone de trente-quatre côtés est x_1, et, pour le construire, on voit qu'il suffit,

1°. De construire deux lignes y et y' telles, que

$$y' - y = 1, \quad yy' = 4;$$

2°. De construire quatre lignes z, z', u, u' telles, que

$$z - z' = y, \quad zz' = 1,$$
$$u' - u = y', \quad uu' = 1;$$

3°. De construire deux lignes x et x_1 telles, que

$$x + x_1 = z, \quad xx_1 = u.$$

Construction. 1°. En un point O d'une ligne indéfinie UV, *fig.* 4, élevons une perpendiculaire OA égale au rayon du cercle, c'est-à-dire à l'unité. Pre ons $OC = \frac{1}{4}$, puis, du point C comme centre, avec CA pour rayon, décrivons un cercle qui coupe en B et D la ligne UV; on aura

$$OB = \frac{1}{2}y, \qquad OD = \frac{1}{2}y';$$

car

$$2OD - 2OB = 4.OC = 1 \quad \text{et} \quad 2OD \times 2OB = 4\overline{OA}^2 = 4.$$

2°. Joignons AB, et du point B comme centre, avec OB pour rayon, décrivons une circonférence qui coupe en M et P la ligne AB prolongée, on aura

$$AM = z, \qquad AP = z';$$

car

$$AM - AP = PM = 2OB = y \quad \text{et} \quad AM.AP = \overline{AO}^2 = 1.$$

Joignons pareillement AD, et du point D comme centre, avec OD pour rayon, décrivons une circonférence qui coupe en N et Q la ligne AD prolongée, on aura

$$AN = u, \quad AQ = u';$$

car

$$AQ - AN = NQ = 2OD = y' \quad \text{et} \quad AN.AQ = \overline{AO}^2 = 1.$$

3°. Rabattons AO en AE sur le prolongement de AD, décrivons sur NE, comme diamètre, un cercle qui coupe AB en F; du point F comme centre, avec $AI = \frac{AM}{2}$ pour rayon, décrivons un cercle qui coupe AD en G; et, enfin, du point G comme centre, avec ce même rayon, décrivons un cercle qui coupe AD en K et H, on aura

$$x_1 = AK, \quad x = AH;$$

car

$$AK + AH = 2GF = 2AI = AM = z$$

et

$$AK.AH = \overline{AF}^2 = AN.AE = AN.AO = u.$$

Le côté du polygone régulier de trente-quatre côtés inscrit dans le cercle dont le rayon est OA, est donc égal à AK.

VINGT-NEUVIÈME LEÇON.

Formule de Lagrange pour le développement de certaines fonctions implicites. — Développement d'une racine de l'équation $z = x + tz^m$. — Autre application de la série de Lagrange.

Formule de Lagrange pour le développement de certaines fonctions implicites.

Lagrange a donné, dans les *Mémoires de l'Académie de Berlin* pour l'année 1768, une formule remarquable par laquelle on peut développer en série une classe étendue de fonctions implicites (*). Laplace a donné ensuite de cette même formule une démonstration très-simple fondée sur le calcul intégral, et que Lagrange a introduite dans sa *Théorie des fonctions analytiques* (**). Plus tard, M. Cauchy en a publié une nouvelle qui a l'avantage de faire connaître le reste de la série (***). Nous présenterons ici la démonstration très-simple et très-directe que M. Duhamel a donnée dans son *Cours de Mécanique de l'École Polytechnique* (****).

Soit une fonction z, d'une variable x, définie par l'équation

$$(1) \qquad z = x + tf(z),$$

où t désigne un paramètre et f une fonction donnée quel-

(*) *Voir* le *Traité de la Résolution des Équations numériques*, Note IX.

(**) *Voir* la 3e édit. de cet ouvrage, que j'ai publiée en 1847, page 147.

(***) *Mémoires de l'Académie royale des Sciences de l'Institut de France*, tome VIII, page 130.

(****) Deuxième partie, page 57.

conque. Nous nous proposons de former le développement de z en série ordonnée suivant les puissances de t.

On a, par la formule de Maclaurin,

$$(2)\quad z = z_0 + \left(\frac{dz}{dt}\right)_0 t + \left(\frac{d^2z}{dt^2}\right)_0 \frac{t^2}{1.2} + \ldots + \left(\frac{d^n z}{dt^n}\right)_0 \frac{t^n}{1.2\ldots n} + R_n,$$

$z_0, \left(\frac{dz}{dt}\right)_0, \ldots, \left(\frac{d^n z}{dt^n}\right)_0$ étant les valeurs de z et de ses dérivées pour $t = 0$, et R_n le reste de la série.

En faisant $t = 0$ dans l'équation (1), on a d'abord

$$z_0 = x;$$

et il ne reste plus qu'à trouver généralement la valeur de $\frac{d^m z}{dt^m}$ pour $t = 0$.

Considérant x et t comme deux variables indépendantes, et différentiant successivement l'équation (1) par rapport à chacune d'elles, on a

$$\frac{dz}{dx} = 1 + tf'(z)\frac{dz}{dx}, \quad \frac{dz}{dt} = f(z) + tf'(z)\frac{dz}{dt};$$

et, en éliminant $f'(z)$,

$$(3)\qquad \frac{dz}{dt} = f(z)\frac{dz}{dx}.$$

Cette équation fait connaître la valeur de $\left(\frac{dz}{dt}\right)_0$, car pour $t = 0$, on a

$$z = z_0 = x \quad \text{et} \quad \frac{dz}{dx} = 1;$$

donc

$$\left(\frac{dz}{dt}\right)_0 = f(x).$$

Pour avoir la valeur de $\left(\frac{d^2z}{dt^2}\right)_0$, différentions l'équa-

tion (3) par rapport à t, et ensuite par rapport à x; on aura

$$\frac{d^2z}{dt^2} = f(z)\frac{d^2z}{dxdt} + f'(z)\frac{dz}{dx}\frac{dz}{dt},$$

$$\frac{d^2z}{dxdt} = f(z)\frac{d^2z}{dx^2} + f'(z)\left(\frac{dz}{dx}\right)^2;$$

en éliminant $\frac{d^2z}{dxdt}$ entre ces équations, et remplaçant $\frac{dz}{dt}$ par sa valeur tirée de (3), il vient

$$\frac{d^2z}{dt^2} = f(z)^2\frac{d^2z}{dx^2} + 2f(z)f'(z)\left(\frac{dz}{dx}\right)^2,$$

et comme le second membre est la dérivée de $f(z)^2\frac{dz}{dx}$ par rapport à x, on aura enfin

$$(4) \qquad \frac{d^2z}{dt^2} = \frac{d\left[f(z)^2\frac{dz}{dx}\right]}{dx}.$$

Faisant maintenant

$$t = 0, \quad z = x, \quad \frac{dz}{dx} = 1,$$

il vient

$$\left(\frac{d^2z}{dt^2}\right)_0 = \frac{df(x)^2}{dx}.$$

On peut continuer de la même manière pour former les dérivées successives $\left(\frac{d^3z}{dt^3}\right)_0$, etc.; mais, pour éviter de répéter sans cesse les mêmes réductions, nous commencerons par établir une formule générale qui simplifiera l'exposition de la méthode.

Soit $\varphi(z)$ une fonction quelconque, et différentions

$$\varphi(z)\frac{dz}{dx},$$

par rapport à t, on aura

$$\frac{d\left[\varphi(z)\frac{dz}{dx}\right]}{dt} = \varphi'(z)\frac{dz}{dt}\frac{dz}{dx} + \varphi(z)\frac{d^2z}{dx\,dt},$$

ou, en mettant à la place de $\frac{dz}{dt}$ et de $\frac{d^2z}{dx\,dt}$ leurs valeurs précédemment écrites,

$$\frac{d\left[\varphi(z)\frac{dz}{dx}\right]}{dt} = [\varphi'(z)f(z) + \varphi(z)f'(z)]\left(\frac{dz}{dx}\right)^2 + \varphi(z)f(z)\frac{d^2z}{dx^2}.$$

Le second membre est la dérivée de

$$\varphi(z)f(z)\frac{dz}{dx},$$

par rapport à x, on aura donc généralement

$$(5)\qquad \frac{d\left[\varphi(z)\frac{dz}{dx}\right]}{dt} = \frac{d\left[\varphi(z)f(z)\frac{dz}{dx}\right]}{dx}.$$

Au moyen de cette formule, on aurait pu déduire l'équation (4) de (3), en supposant $\varphi(z) = f(z)$.

Faisons maintenant $\varphi(z) = f(z)^2$, l'équation (5) donnera

$$\frac{d\left[f(z)^2\frac{dz}{dx}\right]}{dt} = \frac{d\left[f(z)^3\frac{dz}{dx}\right]}{dx},$$

et par conséquent, en différentiant l'équation (4) par rapport à t, on aura

$$\frac{d^3z}{dt^3} = \frac{d^2\left[f(z)^3\frac{dz}{dx}\right]}{dx^2};$$

en différentiant cette dernière par rapport à t, et se ser-

vant de l'équation (5) où l'on fera $\varphi(z) = f(z)^3$, on aura

$$\frac{d^4 z}{dt^4} = \frac{d^3\left[f(z)^4 \frac{dz}{dx}\right]}{dx^3};$$

et je dis que généralement

$$\frac{d^m z}{dt^m} = \frac{d^{m-1}\left[f(z)^m \frac{dz}{dx}\right]}{dx^{m-1}}. \tag{6}$$

Comme nous avons établi cette formule pour les valeurs 1, 2, 3 de m, il suffit de démontrer que si elle a lieu pour une valeur quelconque de m, elle a lieu aussi pour cette même valeur de m augmentée d'une unité. Supposons donc que l'équation (6) ait lieu, et faisons $\varphi(z) = f(z)^m$ dans l'équation (5), on aura

$$\frac{d\left[f(z)^m \frac{dz}{dx}\right]}{dt} = \frac{d\left[f(z)^{m+1} \frac{dz}{dx}\right]}{dx};$$

différentions maintenant l'équation (6) par rapport à t, il vient

$$\frac{d^{m+1} z}{dt^{m+1}} = \frac{d^m\left[f(z)^{m+1} \frac{dz}{dx}\right]}{dx^m},$$

équation qui se déduit de (6) en changeant m en $m+1$. L'équation (6) est donc générale, et en y faisant $t = 0$, il vient

$$\left(\frac{d^m z}{dt^m}\right)_0 = \frac{d^{m-1} f(x)^m}{dx^{m-1}}.$$

Le développement (2) de z sera donc

$$z = x + t f(x) + \frac{t^2}{1.2}\frac{df(x)^2}{dx} + \ldots + \frac{t^n}{1.2\ldots n}\frac{d^{n-1} f(x)^n}{dx^{n-1}} + R_n. \tag{7}$$

Proposons-nous maintenant de former le développement

d'une fonction quelconque $F(z)$ de z en série ordonnée suivant les puissances croissantes de t.

On a, par la formule de Maclaurin,

$$(8)\quad \left\{\begin{array}{l} F(z) = F_0 + \left(\frac{dF}{dt}\right)_0 t + \left(\frac{d^2F}{dt^2}\right)_0 \frac{t^2}{1.2} + \ldots \\ \quad + \left(\frac{d^nF}{dt^n}\right)_0 \frac{t^n}{1.2.3\ldots} + R_n, \end{array}\right.$$

en désignant par F_0, $\left(\frac{dF}{dt}\right)_0$, etc., les valeurs de F et de ses dérivées pour $t = 0$, et par R_n le reste de la série. Le premier terme F_0 est égal à $F(x)$; car on a $z = x$ pour $t = 0$; il reste donc à déterminer généralement $\left(\frac{d^mF}{dt^m}\right)_0$.

On a d'abord

$$\frac{dF}{dt} = F'(z)\frac{dz}{dt} = F'(z)f(z)\frac{dz}{dx},$$

et, en différentiant par rapport à t,

$$\frac{d^2F}{dt^2} = \frac{d\left[F'(z)f(z)\frac{dz}{dx}\right]}{dt};$$

mais l'équation (5) donne, en faisant $\varphi(z) = F'(z)f(z)$,

$$\frac{d\left[F'(z)f(z)\frac{dz}{dx}\right]}{dt} = \frac{d\left[F'(z)f(z)^2\frac{dz}{dx}\right]}{dx};$$

donc

$$\frac{d^2F}{dt^2} = \frac{d\left[F'(z)f(z)^2\frac{dz}{dx}\right]}{dx}.$$

On déduira pareillement de cette dernière, en faisant usage de l'équation (5),

$$\frac{d^3F}{dt^3} = \frac{d^2\left[F'(z)f(z)^3\frac{dz}{dx}\right]}{dx^2},$$

et l'on ferait voir, comme précédemment, qu'on a généralement

$$\frac{d^m F}{dt^m} = \frac{d^{m-1}\left[F'(z) f(z)^m \frac{dz}{dx}\right]}{dx^{m-1}}; \tag{9}$$

faisant $t = 0$, $z = x$, $\frac{dz}{dx} = 1$, cette formule donne

$$\left(\frac{d^m F}{dt^m}\right)_0 = \frac{d^{m-1}[F'(x) f(x)^m]}{dx^{m-1}}.$$

Le développement (8) de $F(z)$ sera, par conséquent,

$$\left\{\begin{aligned} F(z) &= F(x) + tF'(x)f(x) + \frac{t^2}{1.2}\frac{d[F'(x)f(x)^2]}{dx} + \ldots \\ &\quad + \frac{t^n}{1.2.3\ldots n}\frac{d^{n-1}[F'(x)f(x)^n]}{dx^{n-1}} + R_n. \end{aligned}\right. \tag{10}$$

Quant à la forme du reste, je ne crois pas devoir en parler ici, et je renverrai le lecteur au Mémoire dans lequel M. Cauchy a développé cette question.

Développement d'une racine de l'équation $z = x + tz^m$.

En faisant $f(z) = z^m$ dans l'équation (7), on a le développement suivant :

$$\begin{aligned} z = x + x^m t + \frac{2m}{1.2}x^{2m-1}t^2 + \frac{3m(3m-1)}{1.2\ 3}x^{3m-2}t^3 + \ldots \\ + \frac{nm(nm-1)\ldots(nm-n+2)}{1\ 2.3\ldots n}x^{nm-n+1}t^n + \ldots, \end{aligned}$$

pour celle des racines de l'équation

$$z = x + tz^m,$$

qui se réduit à x pour $t = 0$.

Le terme général u_n de cette série a pour valeur

$$u_n = \frac{nm(nm-1)\ldots(nm-n+2)}{1.2.3\ldots n}x^{nm-n+1}t^n;$$

et on en déduit

$$\frac{u_{n+1}}{u_n} = \frac{1}{n+1} \frac{(nm+m)(nm+m-1)\ldots(nm+1)}{(nm-n+2)\ldots(nm-n+m)} x^{m-1} t:$$

pour de très-grandes valeurs de n, ce rapport est à peu près égal à

$$\frac{m^m}{(m-1)^{m-1}} x^{m-1} t.$$

Il en résulte que la série précédente sera convergente, si cette quantité est inférieure à l'unité.

Autre application de la série de Lagrange.

La formule de Lagrange, appliquée à l'équation

$$(1) \qquad z = \zeta + t f(z),$$

où ζ et t sont deux variables, dont la seconde est supposée assez petite pour la convergence de la série, nous donne

$$F(z) = \sum \frac{t^n}{1.2\ldots n} \frac{d^{n-1}[F'(\zeta) f(\zeta)^n]}{d\zeta^{n-1}},$$

et, en différentiant par rapport à ζ,

$$(2) \qquad F'(z)\frac{dz}{d\zeta} = \sum \frac{t^n}{1.2\ldots n} \frac{d^n[F'(\zeta) f(\zeta)^n]}{d\zeta^n}.$$

Maintenant soient

$$F'(z) = z^m \quad \text{et} \quad f(z) = z - 1,$$

l'équation (1) donnera

$$z = \frac{\zeta - t}{1 - t}, \quad \frac{dz}{d\zeta} = \frac{1}{1-t},$$

et, par suite, l'équation (2) devient

$$\frac{(\zeta - t)^m}{(1-t)^{m+1}} = \sum \frac{t^n}{1.2\ldots n} \frac{d^n \zeta^m (\zeta - 1)^n}{d\zeta^n}.$$

Nous ferons usage de cette formule dans la leçon suivante.

TRENTIÈME LEÇON.

Solution d'un problème d'analyse indeterminée relatif à la représentation géométrique des fonctions elliptiques.

La question que je vais développer dans cette leçon est extraite du Mémoire *sur la représentation géométrique des fonctions elliptiques et ultrà elliptiques*, que j'ai publié dans les tomes X et XI du Journal de M. Liouville, et qui fait aussi partie du tome XI du *Recueil des Savants étrangers*.

Problème d'analyse indéterminée.

Trouver toutes les solutions que peut admettre l'équation indéterminée

$$(1) \qquad dx^2 + dy^2 = \frac{c^2 dz^2}{(z^2 - a^2)(z^2 - \alpha^2)},$$

où c est une constante réelle, a et α deux constantes imaginaires conjuguées, en ne prenant pour x et y que des fonctions réelles et rationnelles de z qui ne puissent être infinies que pour $z = \pm a$ et $z = \pm \alpha$.

Désignons, pour abréger, par i l'imaginaire $\sqrt{-1}$. L'équation (1) peut s'écrire de la manière suivante :

$$(2) \qquad \frac{\dfrac{dx + i\,dy}{c\,dz}}{z^2 - a^2} \cdot \frac{\dfrac{dx - i\,dy}{c\,dz}}{z^2 - \alpha^2} = 1;$$

et comme x et y sont des fonctions réelles et rationnelles de z, les deux facteurs du premier membre de l'équation (2) sont des fonctions rationnelles imaginaires et

conjuguées, ayant pour module l'unité. Donc, en désignant par p et ϖ deux polynômes imaginaires et conjugués, par ω un angle réel et par e la base des logarithmes népériens, on pourra poser

$$\frac{\frac{dx+idy}{cdz}}{z^2-a^2}=e^{\omega i}\frac{p}{\varpi},\quad \frac{\frac{dx-idy}{cdz}}{z^2-\alpha^2}=e^{-\omega i}\frac{\varpi}{p},$$

ou

$$(3)\quad \begin{cases} dx+i\,dy = ce^{\omega i}\dfrac{p\,dz}{\varpi(z^2-a^2)}, \\ dx-i\,dy = ce^{-\omega i}\dfrac{\varpi\,dz}{p(z^2-\alpha^2)}. \end{cases}$$

La seconde de ces équations (3) se déduisant de la première par le changement de i en $-i$, il est inutile de la considérer; en intégrant la première, on a

$$(4)\quad x+iy=ce^{\omega i}\int\frac{p}{\varpi}\frac{dz}{z^2-a^2},$$

et il ne reste plus qu'à déterminer les polynômes p et ϖ, de manière que l'intégrale du second membre soit algébrique; car, cela fait, on égalera x à la partie réelle du second membre, y au coefficient de i, et le problème sera résolu.

D'après l'énoncé du problème, x et y ne doivent être infinies que pour $z=\pm a$, $z=\pm\alpha$, il en est donc de même de $x+iy$ et de $x-iy$; par conséquent, le dénominateur ϖ de la quantité sous le signe $\int$ ne peut contenir que les facteurs linéaires

$$z+a,\quad z-a,\quad z+\alpha,\quad z-\alpha,$$

et il en est de même du polynôme conjugué p; d'où il suit que p contient deux de ces quatre facteurs, et que ϖ contient leurs conjugués le même nombre de fois respec-

tivement. On peut faire quatre hypothèses :

1°. $p = (z-\alpha)^m (z+\alpha)^n, \quad \varpi = (z-a)^m (z+a)^n$;
2°. $p = (z-a)^m (z+\alpha)^n, \quad \varpi = (z-\alpha)^m (z+a)^n$;
3°. $p = (z-a)^m (z+a)^n, \quad \varpi = (z-\alpha)^m (z+\alpha)^n$;
4°. $p = (z-\alpha)^m (z+a)^n, \quad \varpi = (z-a)^m (z+\alpha)^n$.

Dans la première hypothèse, on a

$$\frac{p}{\varpi}\frac{dz}{z^2-a^2} = \frac{(z-\alpha)^m (z+\alpha)^n}{(z-a)^{m+1}(z+a)^{n+1}}dz;$$

dans la seconde,

$$\frac{p}{\varpi}\frac{dz}{z^2-a^2} = \frac{(z-a)^{m-1}(z+\alpha)^n}{(z-\alpha)^m (z+a)^{n+1}}dz;$$

ou, en changeant m en $m+1$,

$$\frac{p}{\varpi}\frac{dz}{z^2-a^2} = \frac{(z-a)^m (z+\alpha)^n}{(z-\alpha)^{m+1}(z+a)^{n+1}}dz.$$

La troisième et la quatrième hypothèse donnent les mêmes valeurs de $\frac{p}{\varpi}\frac{dz}{z^2-a^2}$, sauf que a et α sont changés l'un dans l'autre, ce qui ne produit que le changement insignifiant de i en $-i$.

De tout cela, il résulte que les fonctions cherchées x et y seront données par l'une des deux équations suivantes :

$$x+iy = ce^{\omega i}\int \frac{(z-\alpha)^m (z+\alpha)^n}{(z-a)^{m+1}(z+a)^{n+1}}dz, \tag{5}$$

$$x+iy = ce^{\omega i}\int \frac{(z-a)^m (z+\alpha)^n}{(z-\alpha)^{m+1}(z+a)^{n+1}}dz. \tag{6}$$

L'équation (6) est comprise dans l'équation (5), si l'on admet des valeurs négatives pour m; elle se déduit, en effet, de l'équation (5) en changeant m en $-(m+1)$.

On obtiendra la condition pour que l'intégrale de l'équation (5) soit algébrique, en se servant du théorème

que nous avons établi dans la septième leçon; mais il convient auparavant de transformer cette intégrale.

Posons

$$\frac{(a+\alpha)^2}{4a\alpha} = \zeta,$$

et prenons à la place de z une autre variable t, telle que

$$\frac{z+\alpha}{z+a} = \frac{a+\alpha}{2a}\,\frac{1}{t},$$

d'où

$$\frac{dz}{(z+a)^2} = \frac{a+\alpha}{2a(\alpha-a)}\,\frac{dt}{t^2};$$

on aura, après quelques réductions faciles,

$$\int \frac{(z-\alpha)^m (z+\alpha)^n}{(z-a)^{m+1}(z+a)^{n+1}}\,dz$$
$$= \frac{-(2\alpha)^m (a+\alpha)^{n-m}}{(2a)^{n+1}} \int \frac{(\zeta-t)^m}{(1-t)^{m+1}\,t^{n+1}}\,dt.$$

Donc, pour que x et y soient algébriques, il faut et il suffit que l'intégrale

$$(7) \qquad \int \frac{(\zeta-t)^m}{(1-t)^{m+1}\,t^{n+1}}\,dt$$

le soit. Il faut donc qu'en développant

$$\frac{(\zeta-t)^m}{(1-t)^{m+1}\,t^{n+1}}$$

en fraction simple, il n'y ait pas de termes contenant en dénominateur la première puissance de $1-t$ ou de t: mais la dernière de ces deux conditions entraîne l'autre, parce que le degré du dénominateur de la fraction rationnelle surpasse au moins de deux unités le degré du numérateur. (*Voir* septième leçon.)

La seule condition, pour que l'intégrale (7) soit algé-

brique, est donc que la $n^{ième}$ dérivée de

$$\frac{(-\zeta t)^m}{(1-t)^{m+1}},$$

soit nulle pour $t=0$, ou que le développement de cette fonction, suivant les puissances de t, ne contienne pas de terme en t^n. D'ailleurs nous avons trouvé, dans la leçon précédente,

$$\frac{(\zeta-t)^m}{(1-t)^{m+1}}=\sum\frac{t^n}{1.2.3\ldots n}\frac{d^n\zeta^m(\zeta-1)^n}{d\zeta^n};$$

la condition que nous cherchons sera donc

$$\frac{d^n\zeta^m(\zeta-1)^n}{d\zeta^n}=0. \tag{8}$$

Cette équation en ζ est du degré m, et ses m racines sont réelles et comprises entre 0 et 1. Ce théorème se démontre immédiatement, en appliquant m fois de suite le théorème de Rolle à l'équation

$$\zeta^m(\zeta-1)^n=0,$$

qui a m racines égales à 0 et n égales à 1.

En désignant par ζ une racine quelconque de l'équation (8), on aura

$$\frac{(a+\alpha)^2}{4a\alpha}=\zeta; \tag{9}$$

on pourra se donner, à volonté, le module ρ des imaginaires a et α, et si l'on pose

$$a\alpha=\rho^2, \tag{10}$$

les équations (9) et (10) détermineront a et α, qui seront bien, en effet, imaginaires et conjuguées, à cause de $\zeta^2<1$.

Considérons maintenant l'équation (6); comme elle se déduit de l'équation (5) en changeant m en $-(m+1)$, on

peut admettre que la condition nécessaire pour que l'intégrale qu'elle contient soit algébrique, se déduit de l'équation (8) par ce même changement. Cette condition sera donc

$$\frac{d^n \frac{(\zeta - 1)^n}{\zeta^{m+1}}}{d\zeta^n} = 0. \qquad (11)$$

Et, en faisant usage du théorème de Rolle, on voit que cette équation a toutes ses racines réelles et plus grandes que 1, en sorte que, si l'on pose

$$\frac{(a+\alpha)^2}{4a\alpha} = \zeta,$$

les quantités a et α ne pourront pas être imaginaires et conjuguées.

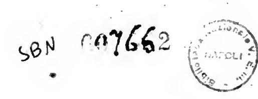
On voit enfin que l'équation (1) ne peut admettre de solutions réelles et rationnelles que celles qui sont données par l'équation (5), où m et n représentent des nombres entiers indéterminés, et encore faut-il, pour qu'elle en admette effectivement, que la quantité

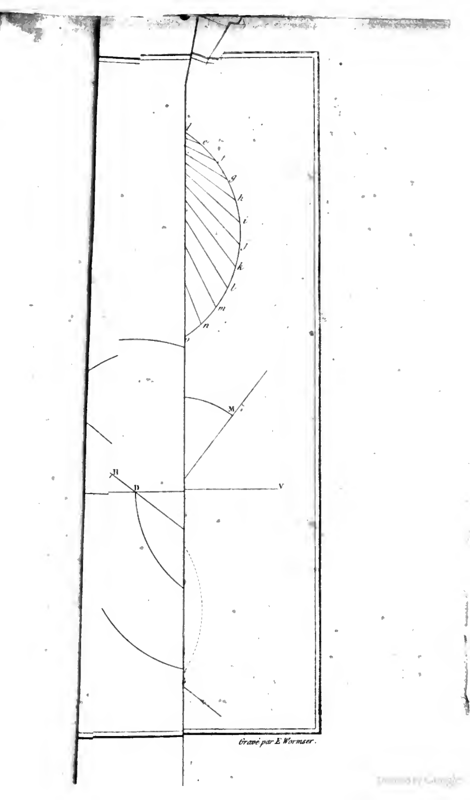
$$\zeta = \frac{(a+\alpha)^2}{4a\alpha}$$

soit une racine de l'équation (8).

Je ne parlerai point ici des applications que j'ai faites des résultats qui précèdent, et je renverrai le lecteur aux divers Mémoires que j'ai publiés sur cette question.

FIN.





Gravé par E. Wormser.


BIBLIOTECA NAZIONALE "VITTORIO EM.LE III"
NAPOLI

